PUBLICAÇÃO ARQUIVADA

A publicação anexa,

Publicação FIPS 180-2

(datado de 1º de agosto de 2002),

foi substituído em 25 de fevereiro de 2004 e é fornecido aqui apenas para fins históricos.

Para a revisão mais atual desta publicação, consulte: http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4.

Informações Federais

Publicação de Padrões de Processamento 180-2

1º de agosto de 2002

Anunciando o

PADRÃO DE HASH SEGURO

As Publicações de Padrões de Processamento de Informações Federais (FIPS PUBS) são emitidas pelo Instituto Nacional de Padrões e Tecnologia (NIST) após a aprovação do Secretário de Comércio de acordo com a Seção 5131 da Lei de Reforma de Gerenciamento de Tecnologia da Informação de 1996 (Lei Pública 104-106), e a Lei de Segurança de Computadores de 1987 (Lei Pública 100-235).

1. Nome do padrão: Secure Hash Signature Standard (SHS) (FIPS PUB 180-2).

2. Categoria do Padrão: Padrão de Segurança de Computadores, Criptografia.

3. Explicação: Este Padrão especifica quatro algoritmos hash seguros - SHA-1, SHA-256, SHA-384 e SHA-512 - para computar uma representação condensada de dados eletrônicos (mensagem). Quando uma mensagem de qualquer comprimento < 264 bits (para SHA-1 e SHA-256) ou < 2128 bits (para SHA-384 e SHA-512) é inserida em um algoritmo, o resultado é uma saída chamada resumo de mensagem.
Os resumos da mensagem variam em comprimento de 160 a 512 bits, dependendo do algoritmo. Algoritmos hash seguros são normalmente usados com outros algoritmos criptográficos, como algoritmos de assinatura digital e códigos de autenticação de mensagem hash com chave, ou na geração de números aleatórios (bits).

Os quatro algoritmos de hash especificados neste padrão são chamados de seguros porque, para um determinado algoritmo, é computacionalmente inviável 1) encontrar uma mensagem que corresponda a um determinado resumo de mensagem ou 2) encontrar duas mensagens diferentes que produzam o mesmo resumo de mensagem . Qualquer alteração em uma mensagem resultará, com uma probabilidade muito alta, em um resumo de mensagem diferente. Isso resultará em uma falha de verificação quando o algoritmo hash seguro for usado com um algoritmo de assinatura digital ou um algoritmo de autenticação de mensagem hash com chave.

Esse padrão substitui o FIPS 180-1, adicionando três algoritmos capazes de produzir resumos de mensagens maiores. O algoritmo SHA-1 especificado aqui é o mesmo algoritmo especificado anteriormente no FIPS 180-1, embora parte da notação tenha sido modificada para ser consistente com a notação usada no SHA-256, SHA-384 e SHA-512 algoritmos.

4. Autoridade de aprovação: Secretário de Comércio.

5. Agência de Manutenção: Departamento de Comércio dos EUA, Instituto Nacional de Padrões e Tecnologia (NIST), Laboratório de Tecnologia da Informação (ITL).

6. Aplicabilidade: Este padrão é aplicável a todos os departamentos e agências federais para a proteção de informações confidenciais não classificadas que não estejam sujeitas à seção 2315 do Título 10, Código dos Estados Unidos ou à seção 3502(2) do Título 44, Código dos Estados Unidos. Este padrão deve ser implementado sempre que um algoritmo de hash seguro for necessário para aplicativos federais, incluindo o uso por outros algoritmos e protocolos criptográficos. A adoção e uso deste padrão está disponível para organizações privadas e comerciais.

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

8. Implementações: Os algoritmos hash seguros aqui especificados podem ser implementados em software, firmware, hardware ou qualquer combinação destes. Somente as implementações de algoritmos validadas pelo NIST serão consideradas em conformidade com este padrão. Informações sobre o programa de validação planejado podem ser obtidas em http://csrc.nist.gov/cryptval/ ou no National Institute of Standards and Technology, Information Technology Laboratory, Attn: SHS Validation, 100 Bureau Drive Stop 8930, Gaithersburg, MD 20899-8930.

9. Cronograma de Implementação: Esta norma entra em vigor em 1º de fevereiro de 2003.

10. Patentes : As implementações dos algoritmos hash seguros neste padrão podem ser cobertas por patentes dos EUA ou estrangeiras.

11. Controle de exportação: Certos dispositivos criptográficos e dados técnicos relacionados a eles estão sujeitos a controles federais de exportação. As exportações de módulos criptográficos que implementam este padrão e os dados técnicos relacionados a eles devem cumprir esses regulamentos federais e ser licenciados pelo Bureau of Export Administration do Departamento de Comércio dos EUA. Os controles de exportação do governo federal aplicáveis são especificados no Título 15, Código de Regulamentos Federais (CFR) Parte 740.17; Título 15, CFR Parte 742; e Título 15, CFR Parte 774, Categoria 5, Parte 2.

12. Qualificações: Embora seja a intenção deste padrão especificar os requisitos gerais de segurança para gerar um resumo de mensagem, a conformidade com este padrão não garante que uma implementação específica seja segura. A autoridade responsável em cada agência ou departamento deve garantir que uma implementação geral forneça um nível aceitável de segurança. Esta norma será revisada a cada cinco anos para avaliar sua adequação.

13. Procedimento de renúncia. Sob certas circunstâncias excepcionais, os chefes das agências federais, ou seus delegados, podem aprovar renúncias aos Padrões Federais de Processamento de Informações (FIPS). Os chefes de tais agências podem redelegar tal autoridade apenas a um funcionário sênior designado de acordo com a Seção 3506(b) do Título 44, Código dos EUA. As renúncias devem ser concedidas somente quando a conformidade com esta norma

a. afetar adversamente o cumprimento da missão de um operador de um computador federal sistema ou
b. causar um grande impacto financeiro adverso no operador que não é compensado pelo governo ampla economia.

Os chefes das agências podem agir de acordo com uma solicitação de isenção por escrito contendo as informações detalhadas acima. Os chefes de agência também podem agir sem um pedido de renúncia por escrito quando determinarem que as condições para atender ao padrão não podem ser atendidas. Os chefes de agência podem aprovar isenções apenas por uma decisão por escrito que explique a base na qual o chefe de agência fez a(s) constatação(ões) necessária(s). Uma cópia de cada uma dessas decisões, com partes confidenciais ou classificadas claramente identificadas, deve ser enviada para: Instituto Nacional de Padrões e Tecnologia; ATTN: FIPS Waiver Decision, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899 8900.

Além disso, uma notificação de cada renúncia concedida e cada delegação de autoridade para aprovar renúncias deve ser enviada imediatamente ao Comitê de Operações Governamentais da Câmara dos Representantes e à Comissão de Assuntos Governamentais do Senado e deve ser publicada prontamente no Federal Register .

Quando a determinação de renúncia se aplica à aquisição de equipamentos e/ou serviços, um aviso da determinação de renúncia deve ser publicado no Commerce Business Daily como parte do aviso de solicitação de ofertas de aquisição ou, se a determinação de renúncia é feita após a publicação desse aviso, por meio de alteração a esse aviso.

Uma cópia da renúncia, quaisquer documentos de suporte, o documento que aprova a renúncia e quaisquer documentos de suporte e anexos, com as exclusões que a agência está autorizada e decide fazer sob a Seção 552(b) do Título 5, Código dos EUA, devem fazer parte da documentação de aquisição e retidos pela agência.

14. Onde obter cópias do padrão: Esta publicação está disponível eletronicamente acessando http://csrc.nist.gov/publications/. Uma lista de outras publicações disponíveis sobre segurança de computadores, incluindo informações sobre pedidos, pode ser obtida na NIST Publications List 91, que está disponível no mesmo site. Como alternativa, cópias das publicações de segurança de computador do NIST estão disponíveis em: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161.

Informações Federais

Publicação de Padrões de Processamento 180-2

1º de agosto de 2002

Especificações para o

PADRÃO DE HASH SEGURO

Índice

1. INTRODUÇÃO 3

2. DEFINIÇÕES 4

2.1 GLOSSÁRIO DE TERMOS E SIGLAS 4
2.2 PARÂMETROS DE ALGORITMO , SÍMBOLOS E TERMOS 4
2.2.1 Parâmetros 4
2.2.2 Símbolos 5

3. NOTAÇÃO E CONVENÇÕES 6

3.1 STRINGS DE BIT E INTEIROS 6
3.2 OPERAÇÕES COM PALAVRAS 7

4. FUNÇÕES E CONSTANTES 9

4.1 FUNÇÕES 9
4.1.1 Funções SHA-1 9
4.1.2 Funções SHA-256 9
4.1.3 Funções SHA-384 e SHA-512 9
4.2 CONSTANTES 10
4.2.1 Constantes SHA-1 10
4.2. 2 Constantes SHA-256 10
4.2.3 SHA-384 e SHA- 512 Constantes 10

5. PRÉ-PROCESSANDO 12

5.1 PREENCHER A MENSAGEM 12
5.1.1 SHA-1 e SHA-256 12
5.1.2 SHA- 384 e SHA-512 12
5.2 ANÁLISE DA MENSAGEM PREENCHIDA 13
5.2.1 SHA-1 e SHA-256 13
5.2.2 SHA-384 e SHA-512 13
5.3 CONFIGURANDO O VALOR DE HASH INICIAL (H(0)) 13
5.3.1 SHA-1 13
5.3.2 SHA-256 13
5.3.3 SHA-384 14
5.3.4 SHA-512 14

6. ALGORITMOS DE HASH SEGUROS 15

6.1 SHA-1 15
6.1.1 Pré-processamento SHA-1 15
6.1.2 Computação de Hash SHA-1 15
6.1.3 Método alternativo para computar um SHA-1 Message Digest 17

6.2 SHA-256..... 18 *6.2.1 Pré-processamento SHA-256*..... *19 6.2.2 Cálculo de Hash SHA-256*..... *19* 6.3 SHA-512..... 20 *6.3.1 Pré-processamento SHA-512*..... *21 6.3.2 Hash SHA-512 Computação*..... *21* 6.4 SHA-384..... 22

APÊNDICE A: SHA -1 EXEMPLOS 25

A.1 EXEMPLO DE SHA-1 (MENSAGEM DE UM BLOCO) ..... 25 A.2 EXEMPLO SHA-1 (MENSAGEM MULTI-BLOCO) ..... 27 A.3 EXEMPLO SHA-1 (MENSAGEM LONGA). 32

APÊNDICE B: SHA -256 EXEMPLOS 33

B.1 EXEMPLO DE SHA-256 (MENSAGEM DE UM BLOCO)..... 33 B.2 EXEMPLO SHA-256 (MENSAGEM MULTI-BLOCO)..... 35 B.3 EXEMPLO DE SHA-256 (MENSAGEM LONGA)..... 40

APÊNDICE C: SHA -512 EXEMPLOS 41

C.1 EXEMPLO DE SHA-512 (MENSAGEM DE UM BLOCO)..... 41 C.2 EXEMPLO SHA-512 (MENSAGEM MULTI-BLOCO)..... 46 C.3 EXEMPLO SHA-512 (MENSAGEM LONGA)..... 55

APÊNDICE D: SHA -384 EXEMPLOS 56

D.1 EXEMPLO DE SHA-384 (MENSAGEM DE UM BLOCO)..... 56 D.2 EXEMPLO SHA-384 (MENSAGEM MULTI-BLOCO)..... 61 D.3 EXEMPLO SHA-384 (MENSAGEM LONGA)..... 70

APÊNDICE E: REFERÊNCIAS 71

1. INTRODUÇÃO Este padrão especifica

quatro algoritmos hash seguros, SHA-11 , SHA-256, SHA-384 e SHA 512. Todos os quatro algoritmos são funções hash iterativas unidirecionais que podem processar uma mensagem para produzir uma representação condensada chamado *resumo de mensagem.* Esses algoritmos permitem a determinação da integridade de uma mensagem: qualquer alteração na mensagem resultará, com uma probabilidade muito alta, em um resumo de mensagem diferente. Esta propriedade é útil na geração e verificação de assinaturas digitais e códigos de autenticação de mensagens, e na geração de números aleatórios (bits).

Cada algoritmo pode ser descrito em dois estágios: pré-processamento e computação de hash.
O pré-processamento envolve preencher uma mensagem, analisar a mensagem preenchida em blocos de m bits e definir valores de inicialização a serem usados no cálculo de hash. A computação de hash gera uma *programação de mensagem* a partir da mensagem preenchida e usa essa programação, junto com funções, constantes e operações de palavra para gerar iterativamente uma série de valores de hash. O valor de hash final gerado pelo cálculo de hash é usado para determinar o resumo da mensagem.

Os quatro algoritmos diferem mais significativamente no número de bits de segurança que são fornecidos para os dados que estão sendo hash - isso está diretamente relacionado ao tamanho do resumo da mensagem. Quando um algoritmo de hash seguro é usado em conjunto com outro algoritmo, pode haver requisitos especificados em outro lugar que exijam o uso de um algoritmo de hash seguro com um certo número de bits de segurança. Por exemplo, se uma mensagem está sendo assinada com um algoritmo de assinatura digital que fornece 128 bits de segurança, esse algoritmo de assinatura pode exigir o uso de um algoritmo hash seguro que também fornece 128 bits de segurança (por exemplo, SHA-256).

Além disso, os quatro algoritmos diferem em termos de tamanho dos blocos e palavras de dados que são usados durante o hash. A Figura 1 apresenta as propriedades básicas de todos os quatro algoritmos de hash seguros.

Algoritmo	Tamanho da Mensagem do (bits)	Tamanho do bloco (bits)	Tamanho da palavra (bits)	Tamanho do resumo da mensagem (bits)	Segurança[2] (bits)
SHA-1[1]	< 2^64	512	32	160	80
SHA-256	< 2^64	512	32	256	128
SHA-384	< 2^128	1024	64	384	192
SHA-512	< 2^128	1024	64	512	256

Figura 1: Propriedades do Algoritmo de Hash Seguro

[1] O algoritmo SHA-1 especificado neste documento é idêntico ao algoritmo SHA-1 especificado no FIPS 180-1 [180 1]. No entanto, esta especificação, FIPS 180-2, usa *ROTLn* (X) em vez de *Sn* (X) [180-1] para denotar “deslocamento circular à esquerda em *n* bits” (ou seja, “rotação à esquerda em *n* bits”). Isso é descrito na Sec. 3.2. Algumas outras alterações de notação foram feitas para serem consistentes com as especificações de SHA-256, SHA-384 e SHA-512.

[2] Nesse contexto, “segurança” refere-se ao fato de que um ataque de aniversário [HAC] em um resumo de mensagem de tamanho *n* produz uma colisão com um fator de trabalho de aproximadamente 2n/2.

2. DEFINIÇÕES

2.1 Glossário de Termos e Siglas

Pedaço	Um dígito binário com um valor de 0 ou 1.
Byte	Um grupo de oito bits.
FIPS	Padrão Federal de Processamento de Informações.
Palavra	Um grupo de 32 bits (4 bytes) ou 64 bits (8 bytes), dependendo do algoritmo de hash seguro.

2.2 Parâmetros, símbolos e termos do algoritmo

2.2.1 Parâmetros

Os parâmetros a seguir são usados nas especificações do algoritmo de hash seguro neste padrão.

a, b, c, …, h Variáveis de trabalho que são as palavras de w bits usadas no cálculo dos valores de hash, *H(i)* .

$H^{(i)}$ o i^{o} valor hash. H(0) é o valor de hash *inicial ; H(N)* é o valor de hash *final* e é usado para determinar o resumo da mensagem.

$H_j^{(i)}$ O j^{a} palavra do *i* valor de hash, onde $H_0^{(i)}$ é a palavra mais à esquerda de hash valor *j* i.

K_t Valor constante a ser usado para iteração *t* do cálculo de hash.

k Número de zeros anexados a uma mensagem durante a etapa de preenchimento.

l Comprimento da mensagem, M, em bits.

m Número de bits em um bloco de mensagem, *M(i).*

M Mensagem a ser hash.

Mi) Bloco de mensagem i, com um tamanho de *m* bits.

$M_j^{(i)}$ O j^{a} palavra do *i* bloco de mensagem, onde $M_0^{(i)}$ é a palavra mais à esquerda de bloco de mensagem *j* i.

n	Número de bits a serem girados ou deslocados quando uma palavra é operada.
N	Número de blocos na mensagem preenchida.
T	Palavra temporária de w-bit usada no cálculo de hash.
Em	Número de bits em uma palavra.
o *t*	o palavra w-bit do agendamento de mensagem.

2.2.2 Símbolos Os

símbolos a seguir são usados nas especificações do algoritmo hash seguro e cada um opera em palavras de w-bit.

1	Operação AND bit a bit.
em	Operação bit a bit OR (“inclusive-OR”).
—	Operação bit a bit XOR (“exclusive-OR”).
	Operação de complemento bit a bit.
+	Módulo de adição *2w* .
<<	Operação de deslocamento à esquerda, onde *x* << *n* é obtido descartando os n bits mais à esquerda da palavra *x* e, em seguida, preenchendo o resultado com *n* zeros à direita.
>>	Operação de deslocamento à direita, onde *x* >> *n* é obtido descartando os *n* bits mais à direita da palavra *x* e, em seguida, preenchendo o resultado com *n* zeros à esquerda.

3. NOTAÇÃO E CONVENÇÕES

3.1 Cadeias de bits e inteiros

A seguinte terminologia relacionada a cadeias de bits e inteiros será usada.

1. Um *dígito hexadecimal* é um elemento do conjunto {0, 1,…, 9, a,…, f}. Um dígito hexadecimal é a representação de uma string de 4 bits. Por exemplo, o dígito hexadecimal “7” representa a string de 4 bits “0111” e o dígito hexadecimal “a” representa a string de 4 bits “1010”.

2. Uma *palavra* é uma string de w bits que pode ser representada como uma sequência de dígitos hexadecimais. Para converter uma palavra em dígitos hexadecimais, cada string de 4 bits é convertida em seu dígito hexadecimal equivalente, conforme descrito em (1) acima. Por exemplo, a string de 32 bits

   1010 0001 0000 0011 1111 1110 0010 0011

   pode ser expresso como “a103fe23” e a string de 64 bits

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

   pode ser expresso como “a103fe2332ef301a”.

   Ao longo desta especificação, a convenção “big-endian” é usada ao expressar palavras de 32 e 64 bits, de modo que dentro de cada palavra, o bit mais significativo seja armazenado na posição de bit mais à esquerda.

3. Um *inteiro* pode ser representado como uma palavra ou par de palavras. Uma representação de palavra em o comprimento da mensagem, l , bits é necessária para as técnicas de preenchimento da Seção 5.1.

   Um inteiro entre 0 e 232-1 *inclusive* pode ser representado como uma palavra de 32 bits. Os quatro bits menos significativos do inteiro são representados pelo dígito hexadecimal mais à direita da representação da palavra. Por exemplo, o inteiro 291 = 28 + 25 + 21 + 20 = 256+32+2+1 é representado pela palavra hexadecimal 00000123.

   O mesmo vale para um inteiro entre 0 e 264-1 *inclusive,* que pode ser representado como uma palavra de 64 bits.

   Se Z é um inteiro, $0 \le Z < 264$, então $Z = 232X + Y$, onde $0 \le X < 232$ e $0 \le Y < 232$.
   Como X e Y podem ser representados como palavras de 32 bits x e y, respectivamente, o inteiro Z pode ser representado como o par de palavras *(x,* y). Esta propriedade é usada para SHA-1 e SHA-256.

Se *Z* é um inteiro, 0 £ *Z* < 2128, então *Z* = 264X + Y, onde 0 £ *X* < 264 e 0 £ *Y* < 264.
Como *X* e *Y* podem ser representados como palavras de 64 bits *x* e y, respectivamente, o inteiro Z pode ser representado como o par de palavras *(x,* y). Esta propriedade é usada para SHA-384 e SHA-512.

4. Para os algoritmos de hash seguro, o tamanho do *bloco de mensagem* - *m* bits - depende do algoritmo.

   a) Para **SHA-1** e **SHA-256,** cada bloco de mensagem possui **512 bits,** que são representados como uma sequência de dezesseis **palavras de 32 bits.**

   b) Para **SHA-384** e **SHA-512,** cada bloco de mensagem possui **1024 bits,** que são representados como uma sequência de dezesseis **palavras de 64 bits.**

3.2 Operações em palavras As seguintes

operações são aplicadas a palavras de w-bit em todos os quatro algoritmos de hash seguros. SHA-1 e SHA-256 operam em palavras de 32 bits *(w* = 32), e SHA-384 e SHA-512 operam em palavras de 64 bits *(w* = 64).

1. Operações de palavras *lógicas* bit a bit : 1, em , — , e (ver Seção 2.2.2).

2. Módulo de adição *2w* .

   A operação *x* + *y* é definida como segue. As palavras *x* e *y* representam os inteiros *X* e Y, onde 0 £ *X* < *2w* e 0 £ *Y* < *2w* . Para inteiros positivos *U* e V, seja *U* modV o resto da divisão *de U* por V. Calcule

   Z = (X + *Y)* mod *2w* .

   Então 0 £ *Z* < *2w* . Converta o inteiro *Z* em uma palavra, z, e defina z = *x* + y.

3. A operação *de deslocamento à direita* ***SHR n(x),*** onde *x* é uma palavra de w bits e *n* é um número inteiro com 0 £ *n* < w, é definido por

   SHR n(x) = *x* >> n.

   Essa operação é usada nos algoritmos SHA-256, SHA-384 e SHA-512.

4. A operação *de rotação à direita* (deslocamento circular à direita) ***ROTR n(x),*** onde *x* é uma palavra de w-bit e *n* é um inteiro com 0 £ *n* < w, é definido por

   ROTRn (x) = *(x* >> n) v *(x* << *w* - n).

   Assim, *ROTR n (x)* é equivalente a um deslocamento circular (rotação) de *x* por *n* posições para o certo.

Essa operação é usada pelos algoritmos SHA-256, SHA-384 e SHA-512.

5. A operação *de rotação à esquerda* (deslocamento circular à esquerda), $ROTL^{n}(x)$, onde *x* é uma palavra de w bits e *n* é um número inteiro com 0 £ *n* < w, é definido por

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

Assim, *ROTL n(x)* é equivalente a um deslocamento circular (rotação) de *x* por *n* posições à esquerda.

Esta operação é usada apenas no algoritmo SHA-1. Observe que na ref. [180-1] esta operação foi referida como “Sn (X)”; no entanto, a notação foi modificada para maior clareza e consistência com a notação usada para operações em outros algoritmos de hash seguros.

6. Observe as seguintes relações de equivalência, onde *w* é fixo em cada relação:

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

$$ROTRn\ (x) = ROTL^{w-n}(x).$$

4. FUNÇÕES E CONSTANTES

4.1 Funções Esta seção

define as funções que são usadas por cada um dos algoritmos. Embora os algoritmos SHA 256, SHA-384 e SHA-512 usem funções semelhantes, suas descrições são separadas em seções para SHA-256 (Seção 4.1.2) e para SHA-384 e SHA-512 (Seção 4.1.2). 3), pois a entrada e a saída dessas funções são palavras de tamanhos diferentes. Cada um dos algoritmos inclui as funções Ch(x, y, z) e Maj(x, y, z); a operação OU exclusivo (¯)nessas funções pode ser substituída por uma operação OU bit a bit (v) e produzir resultados idênticos.

4.1.1 Funções SHA-1

SHA-1 usa uma sequência de funções lógicas, f0, f1,…, f79. Cada função ft, onde 0 £ *t* < 79, opera em três palavras de 32 bits, x, y e z, e produz uma palavra de 32 bits como saída. A função *ft (x,* y, z) é definida da seguinte forma:

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

4.1.2 Funções SHA-256

SHA-256 usa seis funções lógicas, onde *cada função opera em palavras de 32 bits,* que são representadas como x, y e z. O resultado de cada função é uma nova palavra de 32 bits.

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

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

$$\ddot{y}_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR13(x) \oplus ROTR22(x) \quad (4.4)$$

$$\ddot{y}_1^{\{256\}}(x) = ROTR6(x) \oplus ROTR11(x) \oplus ROTR25(x) \quad (4.5)$$

$$x = ROTR7(x) \oplus ROTR18(x) \oplus SHR^3(x) \quad (4.6)$$

$$s_0^{\{256\}} = x = ROTR17(x) \oplus ROTR19(x) \oplus SHR^{10}(x) \quad (4.7)$$

$$s_1^{\{256\}}$$

4.1.3 Funções SHA-384 e SHA-512

SHA-384 e SHA-512 usam cada um seis funções lógicas, onde *cada função opera em palavras de 64 bits,* que são representadas como x, y e z. O resultado de cada função é uma nova palavra de 64 bits.

$$Ch(x, y, z) = (x \wedge y) \oplus (x \wedge z) \tag{4.8}$$

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \tag{4.9}$$

$$\sum_0^{\{512\}}(x) = ROTR28(x) \oplus ROTR34(x) \oplus ROTR39(x) \quad \sum_1^{\{512\}}(x) = ROTR14(x) \oplus ROTR18(x) \oplus ROTR41(x) \tag{4.10}$$

$$\sigma_0^{\{512\}}(x) = ROTR1(x) \oplus ROTR8(x) \oplus SHR^7(x) \tag{4.11}$$

$$\sigma_1^{\{512\}}(x) = ROTR19(x) \oplus ROTR61(x) \oplus SHR^6(x) \tag{4.12}$$

4.2 Constantes

4.2.1 Constantes SHA-1

SHA-1 usa uma sequência de oitenta palavras constantes de 32 bits, K0, K1,…, K79, que são dadas por

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

4.2.2 Constantes SHA-256

SHA-256 usa uma sequência de sessenta e quatro palavras constantes de 32 bits, $k_0^{\{256\}}, k_1^{\{256\}}, \ldots, k_{63}^{\{256\}}$. Esses palavras K representam os primeiros trinta e dois bits das partes fracionárias das raízes cúbicas dos primeiros sessenta e quatro números primos. Em hex, essas palavras constantes são (da esquerda para a direita)

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 Constantes SHA-384 e SHA-512

SHA-384 e SHA-512 usam a mesma sequência de oitenta palavras constantes de 64 bits, $K_0^{\{512\}}, K_1^{\{512\}}, \ldots, K_{79}^{\{512\}}$. Essas palavras representam os primeiros sessenta e quatro bits das partes fracionárias das raízes cúbicas dos primeiros oitenta números primos. Em hex, essas palavras constantes são (da esquerda para a direita)

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. PRÉ-PROCESSAMENTO

O pré-processamento deve ocorrer antes do início da computação de hash. Esse pré-processamento consiste em três etapas: preenchimento da mensagem, *M* (Seção 5.1), análise da mensagem preenchida em blocos de mensagem (Seção 5.2) e definição do valor hash inicial, H(0) (Seção 5.3).

5.1 Preenchendo a mensagem A

mensagem, M, deve ser preenchida antes do início da computação de hash. O objetivo desse preenchimento é garantir que a mensagem preenchida seja um múltiplo de 512 ou 1024 bits, dependendo do algoritmo.

5.1.1 SHA-1 e SHA-256

Suponha que o comprimento da mensagem, M, seja de l bits. Acrescente o bit “1” ao final da mensagem, seguido por *k* bits zero, onde *k* é a menor solução não negativa para a equação l + 1 + *k* ” 448mod 512 . Em seguida, anexe o bloco de 64 bits que é igual ao número l expresso usando uma representação binária. Por exemplo, a mensagem **“abc” (8** bits ASCII) tem comprimento 8 · 3 = 24, então a mensagem é preenchida com um bit, então 448 - (24 +1) = 423 zero bits, e então o comprimento da mensagem , para se tornar a mensagem preenchida de 512 bits

423 64

678 64748

01100001 01100010 01100011 1 00…00 00…011000 .

14243 14243 14243 123

"a" "b" “c” l = 24

O comprimento da mensagem preenchida agora deve ser um múltiplo de 512 bits.

5.1.2 SHA-384 e SHA-512

Suponha que o comprimento da mensagem M, em bits, seja l bits. Acrescente o bit “1” ao final da mensagem, seguido por *k* bits zero, onde *k* é a menor solução não negativa da equação l + 1 + *k* ” 896mod1024. Em seguida, anexe o bloco de 128 bits que é igual ao número l expresso usando uma representação binária. Por exemplo, a mensagem **“abc” (8** bits ASCII) tem comprimento 8 · 3 = 24, então a mensagem é preenchida com um bit, então 896 - (24 + 1) = 871zero bits, e então o comprimento da mensagem, para se tornar a mensagem

preenchida de 1024 bits 128 871

678 64748

01100001 01100010 01100011 1 00…00 00…011000 .

14243 14243 14243 123

"a" "b" “c” l = 24

O comprimento da mensagem preenchida agora deve ser um múltiplo de 1024 bits.

5.2 Analisando a mensagem preenchida Depois
que uma mensagem foi preenchida, ela deve ser analisada em *N* blocos de m bits antes que o cálculo do hash possa começar.

5.2.1 SHA-1 e SHA-256 Para

SHA-1 e SHA-256, a mensagem preenchida é analisada em *N* blocos de 512 bits, M(1) , M(2),…, *M(N)*. Como os 512 bits do bloco de entrada podem ser expressos como dezesseis palavras de 32 bits, os primeiros 32 bits do bloco de mensagem *i* são denotados por $M_0^{(i)}$, os próximos 32 bits são $M_1^{(i)}$, e assim por diante até $M_{15}^{(i)}$.

5.2.2 SHA-384 e SHA-512

Para SHA-384 e SHA-512, a mensagem preenchida é analisada em *N* blocos de 1024 bits, M(1), M(2),…, *M(N)*. Como os 1024 bits do bloco de entrada podem ser expressos como dezesseis palavras de 64 bits, os primeiros 64 bits do bloco de mensagem *i* são denotados $M_0^{(i)}$, os próximos 64 bits são $M_1^{(i)}$, e assim por diante até $M_{15}^{(i)}$.

5.3 Configurando o Valor de Hash Inicial (H(0))

Antes do início da computação de hash para cada um dos algoritmos de hash seguros, o valor de hash inicial, H(0), deve ser definido. O tamanho e o número de palavras em H(0) dependem do tamanho do resumo da mensagem.

5.3.1 SHA-1 Para

SHA-1, o valor de hash inicial, H(0), deve consistir nas seguintes cinco palavras de 32 bits, em hexadecimal:

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

5.3.2 SHA-256

Para SHA-256, o valor de hash inicial, H(0), deve consistir nas seguintes oito palavras de 32 bits, em hexadecimal:

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

Essas palavras foram obtidas tomando os primeiros trinta e dois bits das partes fracionárias das raízes quadradas dos oito primeiros números primos.

5.3.3 SHA-384

Para SHA-384, o valor de hash inicial, H(0), deve consistir nas seguintes oito palavras de 64 bits, em hexadecimal:

$$H_0^{(0)} = \text{cbbb9d5dc1059ed8}$$
$$H1^{(0)} = \text{629a292a367cd507}$$
$$H2^{(0)} = \text{9159015a3070dd17}$$
$$H_3^{(0)} = \text{152fecd8f70e5939}$$
$$H4^{(0)} = \text{67332667ffc00b31}$$
$$H5^{(0)} = \text{8eb44a8768581511}$$
$$H_6^{(0)} = \text{db0c2e0d64f98fa7}$$
$$H_7^{(0)} = \text{47b5481dbefa4fa4}.$$

Essas palavras foram obtidas tomando os primeiros sessenta e quatro bits das partes fracionárias das raízes quadradas do nono ao décimo sexto números primos.

5.3.4 SHA-512

Para SHA-512, o valor de hash inicial, H(0), deve consistir nas seguintes oito palavras de 64 bits, em hexadecimal:

$$H_0^{(0)} = \text{6a09e667f3bcc908}$$
$$H1^{(0)} = \text{bb67ae8584caa73b}$$
$$H2^{(0)} = \text{3c6ef372fe94f82b}$$
$$H_3^{(0)} = \text{a54ff53a5f1d36f1}$$
$$H4^{(0)} = \text{510e527fade682d1}$$
$$H_5^{(0)} = \text{9b05688c2b3e6c1f}$$
$$H_6^{(0)} = \text{1f83d9abfb41bd6b}$$
$$H_7^{(0)} = \text{5be0cd19137e2179}.$$

Essas palavras foram obtidas tomando os primeiros sessenta e quatro bits das partes fracionárias das raízes quadradas dos oito primeiros números primos.

6. ALGORITMOS DE HASH SEGUROS

Nas seções a seguir, SHA-512 é descrito antes de SHA-384. Isso ocorre porque o algoritmo SHA-384 é idêntico ao SHA-512, com exceção de usar um valor de hash inicial diferente e truncar o valor de hash final para 384 bits.

Para cada um dos algoritmos de hash seguros, podem existir métodos de computação alternativos que produzem resultados idênticos; um exemplo é o cálculo SHA-1 alternativo descrito na Seção 6.1.3.
Esses métodos alternativos podem ser implementados em conformidade com este padrão.

6.1 SHA-1

264 SHA-1 pode ser usado para hash de uma mensagem, M, com um comprimento de l bits, onde 0 £ l < . O algoritmo usa 1) uma programação de mensagem de oitenta palavras de 32 bits, 2) cinco variáveis de trabalho de 32 bits cada e 3) um valor de hash de cinco palavras de 32 bits. O resultado final do SHA-1 é um resumo de mensagem de 160 bits.

As palavras da programação de mensagens são rotuladas como W0, W1,…, W79. As cinco variáveis de trabalho são *(i)* rotuladas como a, b, c, d e e. As palavras do valor de hash são rotuladas $_{0}$, $H_{1}^{(eu)}$ .K. $H_{4}^{(eu)}$, qual será H mantêm o valor de hash inicial, H(0), substituído por cada valor de hash intermediário sucessivo (depois que cada bloco de mensagem é , e terminando com o valor de hash final, *H(N)* . SHA-1 também usa um processado), *H(i)* palavra temporária única, T.

O Apêndice A fornece vários exemplos detalhados de SHA-1.

6.1.1 Pré-processamento SHA-1

1. Pad a mensagem, M, de acordo com a Sec. 5.1.1;

2. Analisar a mensagem preenchida em *N* blocos de mensagem de 512 bits, M(1), M(2) de , …, *M(N)*, acordo com a Sec. 5.2.1; e

3. Defina o valor de hash inicial, H(0), conforme especificado na Seção 5.3.1.

6.1.2 Cálculo de hash SHA-1 O cálculo de
hash SHA-1 usa funções e constantes previamente definidas na Seção. 4.1.1 e Sec. 4.2.1, respectivamente. A adição (+) é realizada módulo 232.

Após a conclusão do pré-processamento, cada bloco de mensagem, , M(2), …, *M(N)*, é processado em ordem, M(1) usando as seguintes etapas:

Para *i* = 1 a N: {

1. Prepare a programação da mensagem, {Wt}:

$$peso = \begin{cases} Monte^{(eu)} & 0 \le t \le 15 \\ ROTL1\,(W_{t-3} \; C \; _{t-8} \; C \; _{t-14} \; \bar{}W_{t-16}) & 16 \le t \le 79 \end{cases}$$

2. Inicialize as cinco variáveis de trabalho, a, b, c, d e e, com (i-1) st valor de hash:

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

$b = H1^{(i-1)}$

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

(i-1) $d = H3$

$e = H4^{(i-1)}$

3. Para t = 0 a 79:

{

$T = ROTL5\,(a) + {}_t(b,c,d) + e + K_t + W_t$

$fe = d$

$d = c$

$c = ROTL30\,(b)$

$b = um$

$a = T$

}

4. Calcule o i o valor de hash intermediário $H(i)$:

$H0^{(eu)} = a + H_0^{(i-1)}$

$H1^{(eu)} = b + H1^{(i-1)}$

$H2^{(eu)} = c + H_2^{(i-1)}$

$H3^{(eu)} = d + H3^{(i-1)}$

$H4^{(i)} = e + H4^{(i-1)}$

}

Depois de repetir as etapas de um a quatro um total de N vezes (ou seja, após processar $M(N)$), o resumo de mensagem de 160 bits resultante da mensagem, M, é

$$H0^{(N)} \| H1^{(N)} \| H2^{(N)} \| H3^{(N)} \| H4^{(N)}.$$

6.1.3 Método alternativo para calcular um resumo de mensagem SHA-1 O método de cálculo de hash SHA-1 descrito na Seção 6.1.2 assume que a programação de mensagens W0, W1,…, W79 é implementada como uma matriz de oitenta palavras de 32 bits. Isso é eficiente do ponto de vista da minimização do tempo de execução, pois os endereços de Wt-3,…, Wt-16 na etapa (2) da Sec. 6.1.2 são facilmente calculados.

No entanto, se a memória for limitada, uma alternativa é considerar *{Wt}* como uma fila circular que pode ser implementada usando uma matriz de dezesseis palavras de 32 bits, W0, W1,…, W15. O método alternativo descrito nesta seção produz o mesmo resumo de mensagem que o método de cálculo SHA-1 descrito na Seção 6.1.2. Embora esse método alternativo economize sessenta e quatro palavras de armazenamento de 32 bits, é provável que aumente o tempo de execução devido ao aumento da complexidade dos cálculos de endereço para { Wt} na etapa (3).

Para este método SHA-1 alternativo, deixe *MASK* = 0000000f (em hex). Como no séc. 6.1.1, a adição é realizada no módulo 232. Supondo que o pré-processamento conforme descrito na Sec. 6.1.1 foi executado, o processamento de *M(i)* é o seguinte:

Para *i* = 1 a N: {

1. Para *t* = 0 a 15: {

Peso = $M_t^{(eu)}$

}

2. Inicialize as cinco variáveis de trabalho, a, b, c, d e e, com o (i-1) º valor de hash:

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

b = $H1^{(i-1)}$

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

(i-1) *d* = H3

e = $H4^{(i-1)}$

3. Para *t* = 0 a 79: {

s = *t* 1 *MÁSCARA*

Se *t* ‡ 16 então

{

$$W_s = ROTL1\ (W_{(s+13)1\ MÁSCARA} \bar{}\ W \bar{}\ W \bar{}\ W\ )_{(s+8)1MASK} \quad _{(s+2)1MASK} \quad s$$

}

T = ROTL5 (a) + pés (b, c, *d) + e + Kt + Ws*

e = d

d = c

c = ROTL30 (b)

b = a

a = T

}

4. Calcule o *i* o valor de hash intermediário *H(i) :*

$H0^{(eu)} = a + H_0^{(i-1)}$

$H1^{(eu)} = b + H1^{(i-1)}$

$H2^{(eu)} = c + H_2^{(i-1)}$

$H3^{(eu)} = d + H3^{(i-1)}$

$H4^{(eu)} = e + H4^{(i-1)}$

}

Depois de repetir as etapas de um a quatro um total de *N* vezes (ou seja, após processar *M(N)),* o resumo de mensagem de 160 bits resultante da mensagem, M, é

$$H0^{(N)} \| H1^{(N)} \| H2^{(N)} \| H3^{(N)} \| H4^{(N)}.$$

6.2 SHA-256

264 SHA-256 pode ser usado para hash de uma mensagem, M, com um comprimento de l bits, onde 0 £ l < . O algoritmo usa 1) uma programação de mensagem de sessenta e quatro palavras de 32 bits, 2) oito variáveis de trabalho de 32 bits cada e 3) um valor de hash de oito palavras de 32 bits. O resultado final do SHA-256 é um resumo de mensagem de 256 bits.

As palavras da programação de mensagens são rotuladas como W0, W1,…, W63. As oito variáveis de trabalho são rotulados como a, b, c, d, e, f, g e h. As palavras do valor de hash são rotuladas como $H_0^{(eu)}, H_1^{(eu)}, \ldots, H7^{(eu)}$, conterá o valor de hash inicial, H(0), substituído por cada valor de hash intermediário sucessivo (após o processamento de cada bloco de mensagem), *H(i)* e terminando com o valor de hash final, *H(N)* 256 também usa duas . BEBIDA palavras temporárias, T1 e T2.

O Apêndice B fornece vários exemplos detalhados de SHA-256.

6.2.1 Pré-processamento SHA-256

1. Preencha a mensagem, M, de acordo com a Sec. 5.1.1;

2. Analisar a mensagem preenchida em *N* blocos de mensagem de 512 bits, M(1), M(2) de , ..., *M(N)*, acordo com a Sec. 5.2.1; e

3. Defina o valor de hash inicial, H(0) , conforme especificado na Sec. 5.3.2.

6.2.2 Computação de hash SHA-256 A

computação de hash SHA-256 usa funções e constantes previamente definidas na Seção. 4.1.2 e Sec. 4.2.2, respectivamente. A adição (+) é realizada módulo 232.

Após a conclusão do pré-processamento, cada bloco de mensagem, , M(2) , ..., *M(N)*, é processado em ordem, M(1) usando as seguintes etapas:

Para *i* = 1 a N: {

1. Prepare a programação da mensagem, {Wt}:

$$peso = \begin{cases} Monte^{(eu)} & 0 \pounds t \pounds 15 \\ s_1^{\{256\}}(EM_{t-2}) + W_{t-7} + s_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \pounds t \pounds 63 \end{cases}$$

2. Inicialize as oito variáveis de trabalho, a, b, c, d, e, f, g e h, com o (i-1)st hash valor:

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

$b = H1^{(i-1)}$

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

(i-1) $d = H3$

$e = H4^{(i-1)}$

$f = H5^{(i-1)}$

$g = H6^{(i-1)}$

$h = H7^{(i-1)}$

3. Para *t* = 0 a 63: {

$T = h + \ddot{y}\ 1^{\{256\}}_{1}(e) + \mathrm{Ch}(e, f, g) + K\ t + \overset{\{256\}}{Wt}$

$T2 = \ddot{y}\ (a)^{\{256\}}_{0} + \mathrm{Maj}(a, b, c)\ h = gg =$

$ff = ee$

$= d +$

$T1\ d$

$= c$

$c = b$

$b = um$

$a = T1 + T2$

}

4. Calcule o *i* o valor de hash intermediário *H(i) :*

$H0^{(eu)} = a + H0^{(i-1)}$

$H1^{(eu)} = b + H1^{(i-1)}$

$H2^{(eu)} = c + H2^{(i-1)}$

$H3^{(eu)} = d + H^{(i-1)}_{3}$

$H4^{(eu)} = e + H4^{(i-1)}$

$H5^{(eu)} = f + H5^{(i-1)}$

$H6^{(eu)} = g + H6^{(i-1)}$

$H7^{(eu)} = h + H7^{(i-1)}$

}

Depois de repetir as etapas de um a quatro um total de *N* vezes (ou seja, após processar *M(N)),* o resumo de mensagem de 256 bits resultante da mensagem, M, é

$$H0^{(N)} \| H1^{(N)} \| H2^{(N)} \| H3^{(N)} \| H4^{(N)} \| H5^{(N)} \| H6^{(N)} \| H7^{(N)}.$$

6.3 SHA-512

2128 SHA-512 pode ser usado para hash de uma mensagem, M, com um comprimento de l bits, onde 0 £ l < . O algoritmo usa 1) uma programação de mensagem de oitenta palavras de 64 bits, 2) oito variáveis de trabalho de 64 bits cada e 3) um valor de hash de oito palavras de 64 bits. O resultado final do SHA-512 é um resumo de mensagem de 512 bits.

As palavras da programação de mensagens são rotuladas como W0, W1,…, W79. As oito variáveis de trabalho são rotuladas como a, b, c, d, e, f, g e h. As palavras do valor de hash são rotuladas como $H^{(eu)}_{0}$, $H^{(eu)}_{1}$, $_{,K,}$ $H^{(eu)}_{7}$, que conterá o valor de hash inicial, H(0), substituído por cada valor de hash intermediário sucessivo

(após o processamento de cada bloco de mensagem), *H(i)* e terminando com o valor de hash final, *H(N)* . BEBIDA 512 também usa duas palavras temporárias, T1 e T2.

O Apêndice C fornece vários exemplos detalhados de SHA-512.

6.3.1 Pré-processamento SHA-512

1. Pad a mensagem, M, de acordo com a Sec. 5.1.2;

2. Analisar a mensagem preenchida em *N* blocos de mensagem de 1024 bits, M(1), M(2) de , …, *M(N)*, acordo com a Sec. 5.2.2; e

3. Defina o valor de hash inicial, H(0), conforme especificado na Seção. 5.3.4.

6.3.2 Computação de hash SHA-512 A

computação de hash SHA-512 usa funções e constantes previamente definidas na Seção. 4.1.3 e Sec. 4.2.3, respectivamente. A adição (+) é realizada módulo 264.

Após a conclusão do pré-processamento, cada bloco de mensagem, , M(2) , …, *M(N)*, é processado em ordem, M(1) usando as seguintes etapas:

Para *i* = 1 a N: {

1. Prepare a programação da mensagem, {Wt}:

$$peso = \begin{cases} Monte^{(eu)} & 0 \pounds t \pounds 15 \\ s_1^{\{512\}}(EM_{t-2}) + W_{t-7} + s_0^{\{512\}}(W_{t-15}) + W_{t-16} & 16 \pounds t \pounds 79 \end{cases}$$

2. Inicialize as oito variáveis de trabalho, a, b, c, d, e, f, g e h, com o (i-1)st hash valor:

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

$b = H1^{(i-1)}$

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

(i-1) $d = H3$

$e = H4^{(i-1)}$

$f = H5^{(i-1)}$

$g = H6^{(i-1)}$

$h = H7^{(i-1)}$

3. Para *t* = 0 a 79:

{

$T = h + \ddot{y}_1^{\{512\}}(e) + Ch(e, f, g) + K_t^{\{512\}} + Peso$

$T2 = \ddot{y}(a) + Maj(a, b, c)$

$h = gg =$

$ff = ee$

$= d +$

T1

$d = c$

$c = b$

$b = um$

$a = T1 + T2$

}

4. Calcule o i^{o} valor de hash intermediário $H(i)$:

$H0^{(eu)} = a + H0^{(i-1)}$

$H1^{(eu)} = b + H1^{(i-1)}$

$H2^{(eu)} = c + H2^{(i-1)}$

$H3^{(eu)} = d + H3^{(i-1)}$

$H4^{(i)} = e + H4^{(i-1)}$

$H5^{(eu)} = f + H5^{(i-1)}$

$H6^{(eu)} = g + H6^{(i-1)}$

$H7^{(eu)} = h + H7^{(i-1)}$

}

Depois de repetir as etapas de um a quatro um total de *N* vezes (ou seja, após processar *M(N)),* o resumo de mensagem de 512 bits resultante da mensagem, M, é

$$H0^{(N)} \| H1^{(N)} \| H2^{(N)} \| H3^{(N)} \| H4^{(N)} \| H5^{(N)} \| H6^{(N)} \| H7^{(N)}.$$

6.4 SHA-384

2128 SHA-384 pode ser usado para hash de uma mensagem, M, com um comprimento de l bits, onde 0 £ l < . O algoritmo é definido exatamente da mesma maneira que SHA-512 (Seção 6.3), com as duas exceções a seguir:

1. O valor de hash inicial, H(0), deve ser definido conforme especificado na Seção. 5.3.3; e

2. O resumo da mensagem de 384 bits é obtido truncando o valor de hash final, *H(N)* , ao seu 384 bits mais à esquerda:

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

O Apêndice D fornece vários exemplos detalhados de SHA-384.

APÊNDICE A: EXEMPLOS SHA-1

Este apêndice é apenas para fins informativos e não é necessário para atender ao padrão.

A.1 Exemplo de SHA-1 (mensagem de um bloco)

Deixe a mensagem, M, ser a string ASCII de 24 bits (l = 24) **"abc** ", que é equivalente à seguinte string binária:

01100001 01100010 01100011.

A mensagem é preenchida anexando um bit "1", seguido por 423 bits "0" e terminando com o valor hexadecimal 00000000 00000018 (a representação de duas palavras de 32 bits do comprimento, 24). Assim, a mensagem preenchida final consiste em um bloco *(N* = 1).

Para SHA-1, o valor de hash inicial, H(0), é

$H0^{(0)}$ = 67452301
$H1^{(0)}$ = efcdab89
$H2^{(0)}$ = 98badcfe
$H3^{(0)}$ = 10325476
$H4^{(0)}$ = c3d2e1f0.

As palavras do bloco de mensagens preenchidas são então atribuídas às palavras W0,…,W15 da programação de mensagens:

W0 = 61626380
W1 = 00000000
W2 = 00000000
W3 = 00000000
W4 = 00000000
W5 = 00000000
W6 = 00000000
W7 = 00000000
W8 = 00000000 W9 = 00000000 W10 = 00000000 W11 = 00000000 W12 = 00000000 W13 = 00000000 W14 = 00000000 W15 = 00000018.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d e ***e*** *após* a passagem *t* do loop “for *t* = 0 to 79” descrito na Seção 6.1.2, etapa 4.

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

t = 3 : *t* =	cdd8e11b	a1390f08	626414db	c045bf0c	59d148c0
4 : 5 *t* = : *t*	cfd499de	cdd8e11b	284e43c2	626414db	c045bf0c
= 6 :	3fc7ca40	cfd499de	f3763846	284e43c2	626414db
	993e30c1	3fc7ca40	b3f52677	f3763846	284e43c2
t = 7 :	9e8c07d4		0ff1f290	b3f52677	f3763846
t = 8 :	4b6ae328	993e30c19e8c07d4	664f8c30	0ff1f290	b3f52677
t = 9 : 10	8351f929	4b6ae328	27a301f5	664f8c30	0ff1f290
t = :	fbda9e89	8351f929	12dab8ca	27a301f5	664f8c30
t = 11 : *t*	63188fe4	fbda9e89	60d47e4a	12dab8ca	27a301f5
= 12 :	4607b664	63188fe4	7ef6a7a2	60d47e4a	12dab8ca
t = 13 :	9128f695	4607b664	18c623f9	7ef6a7a2	60d47e4a
t = 14:	196bee77	9128f695	1181ed99	18c623f9	7ef6a7a2
15 *t* = : *t*	20bdd62f	196bee77	644a3da5	1181ed99	18c623f9
= 16 : *t* =	4e925823	20bdd62f	c65afb9d	644a3da5	1181ed99
17 : *t* = 18 :	82aa6728	4e925823	c82f758b	c65afb9d	644a3da5
	dc64901d	82aa6728	d3a49608	c82f758b	c65afb9d
t = 19:	fd9e1d7d	dc64901d	20aa99ca	d3a49608	c82f758b
t = 20 :	1a37b0ca	fd9e1d7d	77192407	20aa99ca	d3a49608
t = 21 : *t*	33a23bfc	1a37b0ca	7f67875f	77192407	20aa99ca
= 22 : *t* =	21283486	33a23bfc	868dez32	7f67875f	77192407
23 : *t* =	d541f12d	21283486	0ce88eff	868dez32	7f67875f
24 :	c7567dc6	d541f12d	884a0d21	0ce88eff	868dez32
t = 25 :	48413ba4	c7567dc6	75507c4b	884a0d21	0ce88eff
t = 26 :	be35fbd5	48413ba4	b1d59f71	75507c4b	884a0d21
t = 27 : *t*	4aa84d97	be35fbd5	12104ee9	b1d59f71	75507c4b
= 28 : *t* =	8370b52e	4aa84d97	6f8d7ef5	12104ee9	b1d59f71
29 : 30	c5fbaf5d	8370b52e	d2aa1365	6f8d7ef5	12104ee9
t = :	1267b407	c5fbaf5d	a0dc2d4b	d2aa1365	6f8d7ef5
t = 31 :	3b845d33	1267b407	717eebd7	a0dc2d4b	d2aa1365
t = 32 :	046faa0a	3b845d33	c499ed01	717eebd7	a0dc2d4b
t = 33 : *t*	2c0ebc11	046faa0a	cee1174c	c499ed01	717eebd7
= 34 : 35 *t*	21796ad4	2c0ebc11	811bea82	cee1174c	c499ed01
= : *t* = 36 :	dcbbb0cb	21796ad4	4b03af04	811bea82	cee1174c
	0f511fd8	dcbbb0cb	085e5ab5	4b03af04	811bea82
t = 37 :	dc63973f	0f511fd8	f72eec32	085e5ab5	4b03af04
t = 38 :	4c986405	dc63973f	03d447f6	f72eec32	085e5ab5
t = 39 : 40	32de1cba	4c986405	f718e5cf	03d447f6	f72eec32
t = *t* :	fc87dedf	32de1cba	53261901	f718e5cf	03d447f6
= 41 : *t* =	970a0d5c	fc87dedf	8cb7872e	53261901	f718e5cf
42 :	7f193dc5	970a0d5c	ff21f7b7	8cb7872e	53261901
t = 43 :	ee1b1aaf	7f193dc5	25c28357	ff21f7b7	
t = 44:	40f28e09	ee1b1aaf	5fc64f71	25c28357	8cb7872eff21f7b7
45 *t* = : *t*	1c51e1f2	40f28e09	fb86c6ab	5fc64f71	25c28357
= 46 : *t* =	a01b846c	1c51e1f2	503ca382	fb86c6ab	5fc64f71
47 : *t* =	conta02ca	a01b846c	8714787c	503ca382	fb86c6ab
48 :	baf39337	conta02ca	2806e11b	8714787c	503ca382
t = 49:	120731c5	baf39337	afab40b2	2806e11b	8714787c
t = 50 :	641db2ce	120731c5	eebce4cd	afab40b2	2806e11b
t = 51 : *t*	3847ad66	641db2ce	4481cc71	eebce4cd	afab40b2
= 52 : *t* =	e490436d	3847ad66	99076cb3	4481cc71	eebce4cd
53 : *t* =	27e9f1d8	e490436d	8e11eb59	99076cb3	4481cc71
54 :	7b71f76d	27e9f1d8	792410db	8e11eb59	99076cb3
t = 55 :	5e6456af	7b71f76d	09fa7c76	792410db	8e11eb59
t = 56 :	c846093f	5e6456af	5edc7ddb	09fa7c76	792410db
t = 57 : *t*	d262ff50	c846093f	d79915ab	5edc7ddb	09fa7c76
= 58 :	09d785fd	d262ff50	f211824f	d79915ab	5edc7ddb

t = 59 : *t*	3f52de5a	09d785fd	3498bfd4	f211824f	d79915ab
= 60 : *t* =	d756c147	3f52de5a	4275e17f	3498bfd4	f211824f
61 : *t* =	548c9cb2	d756c147	8fd4b796	4275e17f	3498bfd4
62 :	b66c020b	548c9cb2	f5d5b051	8fd4b796	4275e17f
t = 63 :	6b61c9e1	b66c020b	9523272c	f5d5b051	8fd4b796
t = 64 :	19dfa7ac	6b61c9e1	ed9b0082	9523272c	f5d5b051
t = 65 : *t*	101655f9	19dfa7ac	5ad87278	ed9b0082	9523272c
= 66 : *t* =	0c3df2b4	101655f9	0677 e9eb	5ad87278	ed9b0082
67 : *t* =	78dd4d2b	0c3df2b4	4405957e	0677 e9eb	5ad87278
68 :	497093c0	78dd4d2b	030pm7cad	4405957e	0677 e9eb
t = 69 :	3f2588c2	497093c0	de37534a	030f7cad	4405957e
t = 70 :	c199f8c7	3f2588c2	125c24f0	de37534a	030f7cad
t = 71 : *t*	39859de7	c199f8c7	8fc96230	125c24f0	de37534a
= 72 : *t* =	edb42de4	39859de7	f0667e31	8fc96230	125c24f0
73 : *t* =	11793f6f	edb42de4	ce616779	f0667e31	8fc96230
74 :	5ee76897	11793f6f	3b6d0b79	ce616779	f0667e31
t = 75 :	63f7dab7	5ee76897	c45e4fdb	3b6d0b79	ce616779
t = 76:	a079b7d9	63f7dab7	d7b9da25	c45e4fdb	3b6d0b79
t = 77 : *t*	860d21cc	a079b7d9	d8fdf6ad	d7b9da25	c45e4fdb
= 78 : *t* =	5738d5e1	860d21cc	681e6df6	d8fdf6ad	d7b9da25
79 :	42541b35	5738d5e1	21834873	681e6df6	d8fdf6ad

Isso completa o processamento do primeiro e único bloco de mensagem, M(1). O valor de hash final, H(1), é calculado para ser

$H_0^{(1)}$ = 67452301 + 42541b35 = a9993e36

$H_1^{(1)}$ = efcdab89 + 5738d5e1 = 4706816a

$H_2^{(1)}$ = 98badcfe + 21834873 = ba3e2571

$H_3^{(1)}$ = 10325476 + 681e6df6 = 7850c26c

$H_4^{(1)}$ = c3d2e1f0 + d8fdf6ad = 9cd0d89d.

O resumo de mensagem de 160 bits resultante é

a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d.

A.2 Exemplo de SHA-1 (mensagem de vários blocos)

Deixe a mensagem, M, ser a string ASCII de 448 bits (l = 448)

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq".

A mensagem é preenchida anexando um bit "1", seguido por 511 bits "0" e terminando com o valor hexadecimal 00000000 000001c0 (a representação de duas palavras de 32 bits do comprimento, 448). Assim, a mensagem preenchida final consiste em dois blocos *(N* = 2).

Para SHA-1, o valor de hash inicial, H(0), é

$H0^{(0)}$ = 67452301

$H1^{(0)}$ = efcdab89

$H2^{(0)}$ = 98badcfe

$H3^{(0)}$ = 10325476

$H4^{(0)}$ = c3d2e1f0.

As palavras do primeiro bloco de mensagem preenchido, M(1), são então atribuídas às palavras W0,…,W15 da programação de mensagem:

W0 = 61626364
W1 = 62636465
W2 = 63646566
W3 = 64.656.667
W4 = 65666768
W5 = 66676869
W6 = 6768696a
W7 = 68696a6b
W8 = 696a6b6c W9 = 6a6b6c6d W10 = 6b6c6d6e W11 = 6c6d6e6f W12 = 6d6e6f70 W13 = 6e6f7071 W14 = 80.000.000 W15 = 00000000.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d e ***e*** *após* a passagem *t* do loop "for *t* = 0 to 79" descrito na Seção 6.1.2, etapa 4.

	a	***b***	***c***	***d***	e
t = 0 :	0116fc17	67452301	7bf36ae2	98badcfe	10325476
t = 1 : *t* =	ebf3b452	0116fc17	59d148c0	7bf36ae2	98badcfe
2 : *t* = 3 :	5109913a	ebf3b452	c045bf05	59d148c0	7bf36ae2
t = 4 :	2c4f6eac	5109913a	bafced14	c045bf05	59d148c0
	33f4ae5b	2c4f6eac	9442644e	bafced14	c045bf05
t = 5 :	96b85189	33f4ae5b	0b13dbab	9442644e	bafced14
t = 6 :	db04cb58	96b85189	ccfd2b96	0b13dbab	9442644e
t = 7 : *t* =	45833f0f	db04cb58	65ae1462	ccfd2b96	0b13dbab
8 : *t* = 9 :	c565c35e	45833f0f	36c132d6	65ae1462	ccfd2b96
t = 10 :	6350afda	c565c35e	d160cfc3	36c132d6	65ae1462
	8993ea77	6350afda	b15970d7	d160cfc3	36c132d6
t = 11 :	e19ecaa2	8993ea77	98d42bf6	b15970d7	d160cfc3
t = 12 :	8603481e	e19ecaa2	e264fa9d	98d42bf6	b15970d7
t = 13 : *t*	32f94a85	8603481e	b867b2a8	e264fa9d	98d42bf6
= 14 : *t* =	b2e7a8be	32f94a85	a180d207	b867b2a8	e264fa9d
15 : *t* =	42637e39	b2e7a8be	4cbe52a1	a180d207	b867b2a8
16 :	6b068048	42637e39	acb9ea2f	4cbe52a1	a180d207
t = 17 :	426b9c35	6b068048	5098df8e	acb9ea2f	4cbe52a1
t = 18 :	944b1bd1	426b9c35	1ac1a012	5098df8e	acb9ea2f
t = 19 : *t*	6c445652	944b1bd1	509ae70d	1ac1a012	5098df8e
= 20 : *t* =	95836da5	6c445652	6512c6f4	509ae70d	1ac1a012
21 : *t* =	09511177	95836da5	9b111594	6512c6f4	509ae70d
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 : *t*	2972f7c7	5a142c1a	bbae0b66	7f48915d	38ae4b71
= 27 : *t* =	d526a644	2972f7c7	96850b06	bbae0b66	7f48915d
28 : *t* =	e1122421	d526a644	ca5cbdf1	96850b06	bbae0b66
29 :	05b457b2	e1122421	3549a991	ca5cbdf1	96850b06
t = 30 :	a9c84bec	05b457b2	78448908	3549a991	ca5cbdf1
t = 31 :	52e31f60	a9c84bec	816d15ec	78448908	3549a991
t = 32 : *t*	5af3242c	52e31f60	2a7212fb	816d15ec	78448908
= 33 : *t* =	31c756a9	5af3242c	14b8c7d8	2a7212fb	816d15ec
34 : *t* =	e9ac987c	31c756a9	16bcc90b	14b8c7d8	2a7212fb
35 :	ab7c32ee	e9ac987c	4c71d5aa	16bcc90b	14b8c7d8
t = 36 :	5933fc99	ab7c32ee	3a6b261f	4c71d5aa	16bcc90b
t = 37 :	43f87ae9	5933fc99	aadf0cbb	3a6b261f	4c71d5aa
t = 38 : *t*	24957f22	43f87ae9	564cff26	aadf0cbb	3a6b261f
= 39 : *t* =	adeb7478	24957f22	50fe1eba	564cff26	aadf0cbb
40 : *t* =	d70e5010	adeb7478	89255fc8	50fe1eba	564cff26
41 :	79bcfb08	d70e5010	2b7add1e	89255fc8	50fe1eba
t = 42 :	f9bcb8de	79bcfb08	35c39404		89255fc8
t = 43 :	633e9561	f9bcb8de	1e6f3ec2	2b7add1e35c39404	2b7add1e
t = 44 : *t*	98c1ea64	633e9561	be6f2e37	1e6f3ec2	35c39404
= 45 : *t* =	c6ea241e	98c1ea64	58cfa558	be6f2e37	1e6f3ec2
46 : *t* =	a2ad4f02	c6ea241e	26307a99	58cfa558	be6f2e37
47 :	c8a69090	a2ad4f02	b1ba8907	26307a99	58cfa558
t = 48 :	88341600	c8a69090	a8ab53c0	b1ba8907	
t = 49 :	7e846f58	88341600	3229a424	a8ab53c0	26307a99b1ba8907
t = 50 : *t*	86e358ba	7e846f58	220d0580	3229a424	a8ab53c0
= 51 : *t* =	8d2e76c8	86e358ba	1fa11bd6	220d0580	3229a424
52 : *t* =	ce892e10	8d2e76c8	a1b8d62e	1fa11bd6	220d0580
53 :	edea95b1	ce892e10	234b9db2	a1b8d62e	1fa11bd6
t = 54 :	36d1230a	edea95b1	33a24b84	234b9db2	a1b8d62e
t = 55 :	776c3910	36d1230a	7b7aa56c	33a24b84	234b9db2
t = 56 : *t*	a681b723	776c3910	8db448c2	7b7aa56c	33a24b84
= 57 : *t* =	ac0a794f	a681b723	1ddb0e44	8db448c2	7b7aa56c
58 : *t* =	f03d3782	ac0a794f	e9a06dc8	1ddb0e44	8db448c2
59 :	9ef775c3	f03d3782	eb029e53	e9a06dc8	1ddb0e44
t = 60 :	36254b13	9ef775c3	bc0f4de0	eb029e53	e9a06dc8
t = 61 :	4080d4dc	36254b13	e7bddd70	bc0f4de0	eb029e53
t = 62 : *t*	2bfaf7a8	4080d4dc	cd8952c4	e7bdd70	bc0f4de0
= 63 : *t* =	513f9ca0	2bfaf7a8	10203537	cd8952c4	e7bdd70
64 : *t* =	e5895c81	513f9ca0	0afebdea	10203537	cd8952c4
65 :	1037d2d5	e5895c81	144fe728	0afebdea	10203537
t = 66 :		1037d2d5	79625720	144fe728	0afebdea
t = 67 :	14a82da96d17c9fd	14a82da9	440df4b5	79625720	144fe728
t = 68 : *t*	2c7b07bd	6d17c9fd	452a0b6a	440df4b5	79625720
= 69 : *t* =	fdf6efff	2c7b07bd	5b45f27f	452a0b6a	440df4b5
70 : *t* =	112b96e3	fdf6efff	4b1ec1ef	5b45f27f	452a0b6a
71 :	84065712	112b96e3	ff7dbbff	4b1ec1ef	5b45f27f
t = 72 :	ab89fb71	84065712	c44ae5b8	ff7dbbff	4b1ec1ef
t = 73 :	c5210e35	ab89fb71	a10195c4	c44ae5b8	ff7dbbff
t = 74 : *t*	352d9f4b	c5210e35	6ae27edc	a10195c4	c44ae5b8
= 75 : *t* =	1a0e0e0a	352d9f4b	7148438d	6ae27edc	a10195c4
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

Isso completa o processamento do primeiro bloco de mensagem, M(1). O primeiro valor de hash intermediário, H(1), é calculado para ser

$H_0^{(1)}$ = 67452301 + 8ce34517 = f4286818

$H_1^{(1)}$ = efcdab89 + d3ad7c25 = c37b27ae

$H_2^{(1)}$ = 98badcfe + 6b4e1883 = 0408f581

$H_3^{(1)}$ = 10325476 + 74351cd2 = 84677148

$H_4^{(1)}$ = c3d2e1f0 + 86838382 = 4a566572.

As palavras do *segundo* bloco de mensagem acolchoado, M(2), são então atribuídas às palavras W0,…,W15 da programação de mensagem:

W0 = 00000000
W1 = 00000000
W2 = 00000000
W3 = 00000000
W4 = 00000000
W5 = 00000000
W6 = 00000000
W7 = 00000000
W8 = 00000000 W9 = 00000000 W10 = 00000000 W11 = 00000000 W12 = 00000000 W13 = 00000000 W14 = 00000000 W15 = 000001c0.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d e ***e*** *após* a passagem *t* do loop "for *t* = 0 to 79" descrito na Seção 6.1.2, etapa 4.

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

t = 22 : *t*	9ad594b9	ee8700bd	cdd20bd7	f6264854	f0badc27
= 23 : *t* =	8fbaa5b9	9ad594b9	7ba1c02f	cdd20bd7	f6264854
24 : *t* =	88fb5867	8fbaa5b9	66b5652e	7ba1c02f	cdd20bd7
25 :	eec50521	88fb5867	63eea96e	66b5652e	7ba1c02f
t = 26 :	50bce434	eec50521	e23ed619	63eea96e	66b5652e
t = 27 :	5c416daf	50bce434	7bb14148	e23ed619	63eea96e
t = 28 : *t*	2429be5f	5c416daf	142f390d	7bb14148	e23ed619
= 29 : *t* =	0a2fb108	2429be5f	d7105b6b	142f390d	7bb14148
30 : *t* =	17986223	0a2fb108	c90a6f97	d7105b6b	142f390d
31 :	8a4af384	17986223	028bec42	c90a6f97	d7105b6b
t = 32 :	6b629993	8a4af384	c5e61888		c90a6f97
t = 33 :	f15f04f3	6b629993	2292bce1	028bec42c5e61888	028bec42
t = 34 : *t*	295cc25b	f15f04f3	pai8a664	2292bce1	c5e61888
= 35 : *t* =	696da404	295cc25b	fc57c13c	pai8a664	2292bce1
36 : *t* =	cef5ae12	696da404	ca573096	fc57c13c	pai8a664
37 :	87d5b80c	cef5ae12	1a5b6901	ca573096	fc57c13c
t = 38 :		87d5b80c	b3bd6b84	1a5b6901	ca573096
t = 39 :	84e2a5f203bb6310	84e2a5f2	21f56e03	b3bd6b84	1a5b6901
t = 40 : *t*	c2d8f75f	03bb6310	a138a97c	21f56e03	b3bd6b84
= 41 : *t* =	bfb25768	c2d8f75f	00eed8c4	a138a97c	21f56e03
42 : *t* =	28589152	bfb25768	f0b63dd7	00eed8c4	a138a97c
43 :	ec1d3d61	28589152	2fec95da	f0b63dd7	00eed8c4
t = 44 :	3caed7af	ec1d3d61	8a162454	2fec95da	f0b63dd7
t = 45 :	c3d033ea	3caed7af	7b074f58	8a162454	2fec95da
t = 46 : *t*	7316056a	c3d033ea	cf2bb5eb	7b074f58	8a162454
= 47 : *t* =	46f93b68	7316056a	b0f40cfa	cf2bb5eb	7b074f58
48 : *t* =	dc8e7f26	46f93b68	9cc5815a	b0f40cfa	cf2bb5eb
49 :	850d411c	dc8e7f26	11be4eda	9cc5815a	b0f40cfa
t = 50 :		850d411c	b7239fc9	11 be4eda	9cc5815a
t = 51 :	7e4672c089fbd41d	7e4672c0	21435047	b7239fc9	11be4eda
t = 52 : *t*	1797e228	89fbd41d	1f919cb0	21435047	b7239fc9
= 53 : *t* =	431d65bc	1797e228	627ef507	1f919cb0	21435047
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 : *t*	5b086c42	e785655a	ea1256a6	db69cb9f	caf6ee32
= 59 : *t* =	a65818f7	5b086c42	b9e15956	ea1256a6	db69cb9f
60 : *t* =	7aab101b	a65818f7	96c21b10	b9e15956	ea1256a6
61 :	93614c9c	7aab101b	e996063d	96c21b10	b9e15956
t = 62 :	f66d9bf4	93614c9c	deaac406	e996063d	96c21b10
t = 63 :	d504902b	f66d9bf4	24d85327	deaac406	e996063d
t = 64 : *t*	60a9da62	d504902b	3d9b66fd	24d85327	deaac406
= 65 : *t* =	8b687819	60a9da62	f541240a	3d9b66fd	24d85327
66 : *t* =	083e90c3	8b687819	982a7698	f541240a	3d9b66fd
67 :	f6226bbf	083e90c3	62da1e06	982a7698	f541240a
t = 68 :	76c0563b	f6226bbf	c20fa430	62da1e06	982a7698
t = 69 :	989dd165	76c0563b	fd889aef	c20fa430	62da1e06
t = 70 : *t*	8b2c7573	989dd165	ddb0158e	fd889aef	c20fa430
= 71 : *t* =	ae1b8e7b	8b2c7573	66277459	ddb0158e	fd889aef
72 : *t* =	ca1840de	ae1b8e7b	e2cb1d5c	66277459	ddb0158e
73 :	16f3babb	ca1840de	eb86e39e	e2cb1d5c	66277459
t = 74 :	d28d83ad	16f3babb	b2861037	eb86e39e	e2cb1d5c
t = 75 :	6bc02dfe	d28d83ad	c5bceaeae	b2861037	eb86e39e
t = 76 : *t*	d3a6e275	6bc02dfe	74a360eb	c5bceaeae	b2861037
= 77 :	da955482	d3a6e275	9af00b7f	74a360eb	c5bceaeae

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

Isso completa o processamento do segundo e último bloco de mensagem, M(2). O valor de hash final, H(2), é calculado para ser

$H_0^{(1)}$ = f4286818 + 906fd62c = 84983e44

$H_1^{(1)}$ = c37b27ae + 58c0aac0 = 1c3bd26e

$H_2^{(1)}$ = 0408f581 + b6a55520 = baae4aa1

$H_3^{(1)}$ = 84677148 + 74e9b89d = f95129e5

$H_4^{(1)}$ = 4a566572 + 9af00b7f = e54670f1.

O resumo de mensagem de 160 bits resultante é

84983e44 1c3bd26e baae4aa1 f95129e5 e54670f1.

A.3 Exemplo de SHA-1 (mensagem longa)

Seja a mensagem *M* a forma codificada em binário da string ASCII que consiste em 1.000.000 de repetições do caractere “a”. O resumo da mensagem SHA-1 resultante é

34aa973c d4c4daa4 f61eeb2b dbad2731 6534016f.

APÊNDICE B: EXEMPLOS SHA-256

Este apêndice é apenas para fins informativos e não é necessário para atender ao padrão.

B.1 Exemplo de SHA-256 (mensagem de um bloco)

Deixe a mensagem, M, ser a string ASCII de 24 bits (l = 24) **"abc** ", que é equivalente à seguinte string binária:

01100001 01100010 01100011.

A mensagem é preenchida anexando um bit "1", seguido por 423 bits "0" e terminando com o valor hexadecimal 00000000 00000018 (a representação de duas palavras de 32 bits do comprimento, 24). Assim, a mensagem preenchida final consiste em um bloco *(N* = 1).

Para SHA-256, o valor de hash inicial, H(0), é

$H0^{(0)}$ = 6a09e667
$H1^{(0)}$ = bb67ae85
$H2^{(0)}$ = 3c6ef372
$H3^{(0)}$ = a54ff53a
$H4^{(0)}$ = 510e527f
$H5^{(0)}$ = 9b05688c
$H6^{(0)}$ = 1f83d9ab
$H7^{(0)}$ = 5be0cd19.

As palavras do bloco de mensagens preenchidas são então atribuídas às palavras W0,…,W15 da programação de mensagens:

W0 = 61626380
W1 = 00000000
W2 = 00000000
W3 = 00000000
W4 = 00000000
W5 = 00000000
W6 = 00000000
W7 = 00000000
W8 = 00000000 W9
= 00000000 W10 =
00000000 W11 =
00000000 W12 =
00000000 W13 =
00000000 W14 =
00000000 W15 =
00000018.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 63" descrito na Seção 6.2.2, etapa 4.

a	b	c	d	e	f	g	h

t = 0 : 5d6aebcd 6a09e667 bb67ae85 3c6ef372 fa2a4622 510e527f 9b05688c 1f83d9ab *t* = : 5a6ad9ad 5d6aebcd 6a09e667 bb67ae85 78ce7989 fa2a4622 510e527f
9b05688c *t* = : c8c347a7 5a6ad9ad 5d6aebcd 6a09e667 f92939eb 78ce7989 fa2a4622 510e527f *t* = : d550f666 c8c347a7 5a6ad9ad 5d6aebcd 24e00850 f92939eb
78ce7989 *t* = : 04409a6a d550f666 c8c347a7 5a6ad9ad 43ada245 24e00850 f92939eb 78ce7989 *t* = : 2b4209f5 04409a6a d550f666 c8c347a7 714260ad
43ada245 24e00850 f92939eb *t* = : e5030380 2b4209f5 04409a6a d550f666 9b27a401 714260ad 43ada245 24e00850 *t* = : 85a07b5f e5030380 2b4209f5 04409a6a
0c657a79 9b27a401 714260ad 43ada245 *t* = : 8e04ecb9 85a07b5f e5030380 2b4209f5 32ca2d8c 0c657a79 9b27a401 714260ad *t* = : 8c87346b 8e04ecb9 85a07b5f
e5030380 1cc92596 32ca2d8c 0c657a79 9b27a401 *t* = : 4798a3f4 8c87346b 8e04ecb9 85a07b5f 436b23e8 1cc92596 32ca2d8c 0c657a79 *t* = : f71fc5a9 4798a3f4
8c87346b 8e04ecb9 816fd6e9 436b23e8 1cc92596 32ca2d8c *t* = : 87912990 f71fc5a9 4798a3f4 8c87346b 1e578218 816fd6e9 436b23e8 1cc92596 *t* = : d932eb16
87912990 f71fc5a9 4798a3f4 745a48de 1e578218 816fd6e9 436b23e8 *t* = : c0645fde d932eb16 87912990 f71fc5a9 0b92f20c 745a48de 1e578218 816fd6e9 *t* = :
b0fa238e c0645fde d932eb16 87912990 07590dcd 0b92f20c 745a48de 1e578218 *t* = : 21da9a9b b0fa238e c0645fde d932eb16 8034229c 07590dcd 0b92f20c 745a48de
t = : c2fbd9d1 21da9a9b b0fa238e c0645fde 846ee454 8034229c 07590dcd 0b92f20c *t* = : fe777bbf c2fbd9d1 21da9a9b b0fa238e cc899961 846ee454 8034229c
07590dcd *t* = : e1f20c33 fe777bbf c2fbd9d1 21da9a9b b0638179 cc899961 846ee454 8034229c *t* = : 9dc68b63 e1f20c33 fe777bbf c2fbd9d1 8ada8930 b0638179
cc899961 846ee454 *t* = : c2606d6d 9dc68b63 e1f20c33 fe777bbf e1257970 8ada8930 b0638179 cc899961 *t* = : a7a3623f c2606d6d 9dc68b63 e1f20c33 49f5114a
e1257970 8ada8930 b0638179 *t* = : c5d53d8d a7a3623f c2606d6d 9dc68b63 aa47c347 49f5114a e1257970 8ada8930 *t* = : 1c2c2838 c5d53d8d a7a3623f c2606d6d
2823ef91 aa47c347 49f5114a e1257970 *t* = : cde8037d 1c2c2838 c5d53d8d a7a3623f 14383d8e 2823ef91 aa47c347 49f5114a *t* = : b62ec4bc cde8037d 1c2c2838
c5d53d8d c74c6516 14383d8e 2823ef91 aa47c347 *t* = : 77d37528 b62ec4bc cde8037d 1c2c2838 edffbff8 c74c6516 14383d8e 2823ef91 *t* = : 363482c9 77d37528
b62ec4bc cde8037d 6112a3b7 edffbff8 c74c6516 14383d8e *t* = : a0060b30 363482c9 77d37528 b62ec4bc ade79437 6112a3b7 edffbff8 c74c6516 *t* = : ea992a22
a0060b30 363482c9 77d37528 0109ab3a ade79437 6112a3b7 edffbff8 *t* = : 73b33bf5 ea992a22 a0060b30 363482c9 ba591112 0109ab3a ade79437 6112a3b7 *t* = :
98e12507 73b33bf5 ea992a22 a0060b30 9cd9f5f6 ba591112 0109ab3a ade79437 *t* = : fe604df5 98e12507 73b33bf5 ea992a22 59249dd3 9cd9f5f6 ba591112 0109ab3a
t = : a9a7738c fe604df5 98e12507 73b33bf5 085f3833 59249dd3 9cd9f5f6 ba591112 *t* = : 65a0cfe4 a9a7738c fe604df5 98e12507 f4b002d6 085f3833 59249dd3 9cd9f5f6
t = : 41a65cb1 65a0cfe4 a9a7738c fe604df5 0772a26b f4b002d6 085f3833 59249dd3 *t* = : 34df1604 41a65cb1 65a0cfe4 a9a7738c a507a53d 0772a26b f4b002d6
085f3833 *t* = : 6dc57a8a 34df1604 41a65cb1 65a0cfe4 f0781bc8 a507a53d 0772a26b f4b002d6 *t* = : 79ea687a 6dc57a8a 34df1604 41a65cb1 1efbc0a0 f0781bc8
a507a53d 0772a26b *t* = : d6670766 79ea687a 6dc57a8a 34df1604 26352d63 1efbc0a0 f0781bc8 a507a53d *t* = : df46652f d6670766 79ea687a 6dc57a8a 838b2711
26352d63 1efbc0a0 f0781bc8 *t* = : 17aa0dfe df46652f d6670766 79ea687a decd4715 838b2711 26352d63 1efbc0a0 *t* = : 9d4baf93 17aa0dfe df46652f d6670766
fda24c2e decd4715 838b2711 26352d63 *t* = : 26628815 9d4baf93 17aa0dfe df46652f a80f11f0 fda24c2e decd4715 838b2711 *t* = : 72ab4b91 26628815 9d4baf93
17aa0dfe b7755da1 a80f11f0 fda24c2e decd4715 *t* = : a14c14b0 72ab4b91 26628815 9d4baf93 d57b94a9 b7755da1 a80f11f0 fda24c2e *t* = : 4172328d a14c14b0
72ab4b91 26628815 fecf0bc6 d57b94a9 b7755da1 a80f11f0 *t* = : 05757ceb 4172328d a14c14b0 72ab4b91 bd714038 fecf0bc6 d57b94a9 b7755da1 *t* = : f11bfaa8
05757ceb 4172328d a14c14b0 6e5c390c bd714038 fecf0bc6 d57b94a9 *t* = : 7a0508a1 f11bfaa8 05757ceb 4172328d 52f1ccf7 6e5c390c bd714038 fecf0bc6 t = :
886e7272 7a0508a1 f11bfaa8 05757ceb 49231c1e 52f8cd7 52f8cd3906bcd3cf7 52f1ccf7 52f1ccf7 52f1ccf7 52f1ccf7 52f1cc39

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

Isso completa o processamento do primeiro e único bloco de mensagem, M(1). O valor de hash final, H(1), é calculado para ser

$H_0^{(1)}$ = 6a09e667 + 506e3058 = ba7816bf

$H1^{(1)}$ = bb67ae85 + d39a2165 = 8f01cfea

$H_2^{(1)}$ = 3c6ef372 + 04d24d6c = 414140de

$H3^{(1)}$ = a54ff53a + b85e2ce9 = 5dae2223

$H_4^{(1)}$ = 510e527f + 5ef50f24 = b00361a3

$H_5^{(1)}$ = 9b05688c + fb121210 = 96177a9c

$H_6^{(1)}$ = 1f83d9ab + 948d25b6 = b410ff61

$H7^{(1)}$ = 5be0cd19 + 961f4894 = f20015ad.

O resumo de mensagem de 256 bits resultante é

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

B.2 Exemplo de SHA-256 (mensagem de vários blocos)

Deixe a mensagem, M, ser a string ASCII de 448 bits (l = 448)

"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq".

A mensagem é preenchida anexando um bit "1", seguido por 511 bits "0" e terminando com o valor hexadecimal 00000000 000001c0 (a representação de duas palavras de 32 bits do comprimento, 448). Assim, a mensagem preenchida final consiste em dois blocos *(N* = 2).

Para SHA-256, o valor de hash inicial, H(0), é

$H0^{(0)}$ = 6a09e667

$H1^{(0)}$ = bb67ae85

$H2^{(0)}$ = 3c6ef372

$H3^{(0)}$ = a54ff53a

$H4^{(0)}$ = 510e527f

$H5^{(0)}$ = 9b05688c

$H6^{(0)}$ = 1f83d9ab

$H7^{(0)}$ = 5be0cd19.

As palavras do primeiro bloco de mensagem preenchido, M(1), são então atribuídas às palavras W0,…,W15 da programação de mensagem:

W0 = 61626364
W1 = 62636465
W2 = 63646566
W3 = 64.656.667
W4 = 65666768
W5 = 66676869
W6 = 6768696a
W7 = 68696a6b
W8 = 696a6b6c W9 = 6a6b6c6d W10 = 6b6c6d6e W11 = 6c6d6e6f W12 = 6d6e6f70 W13 = 6e6f7071 W14 = 80.000.000 W15 = 00000000.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 63" descrito na Seção 6.2.2, etapa 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

Isso completa o processamento do primeiro bloco de mensagem, M(1). O primeiro valor de hash intermediário, H(1), é calculado para ser

$H_0^{(1)}$ = 6a09e667 + 1bdc6f6f = 85e655d6

$H_1^{(1)}$ = bb67ae85 + 86126910 = 417a1795

$H_2^{(1)}$ = 3c6ef372 + f6f443f8 = 3363376a

$H_3^{(1)}$ = a54ff53a + bcfce922 = 624cde5c

$H_4^{(1)}$ = 510e527f + 25d2430a = 76e09589

$H_5^{(1)}$ = 9b05688c + 2fc08f85 = cac5f811

$H_6^{(1)}$ = 1f83d9ab + acc75916 = cc4b32c1

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

As palavras do *segundo* bloco de mensagem acolchoado, M(2), são então atribuídas às palavras W0,…,W15 da programação de mensagem:

W0 = 00000000
W1 = 00000000
W2 = 00000000
W3 = 00000000
W4 = 00000000
W5 = 00000000
W6 = 00000000
W7 = 00000000
W8 = 00000000 W9 = 00000000 W10 = 00000000 W11 = 00000000 W12 = 00000000 W13 = 00000000 W14 = 00000000 W15 = 000001c0.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 63" descrito na Seção 6.2.2, etapa 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

Isso completa o processamento do segundo e último bloco de mensagem, M(2). O valor de hash final, H(2), é calculado para ser

$H_0^{(2)}$ = 85e655d6 + 9ea7148b = 248d6a61

$H1^{(2)}$ = 417a1795 + 908c2123 = d20638b8

$H2^{(2)}$ = 3363376a + b25cef29 = e5c02693

$H_3^{(2)}$ = 624cde5c + a9f181dd = 0c3e6039

$H4^{(2)}$ = 76e09589 + 2c5c4ed0 = a33ce459

$H5^{(2)}$ = cac5f811 + 9a392956 = 64ff2167

$H_6^{(2)}$ = cc4b32c1 + 2aa1bb13 = f6ecedd4

$H_7^{(2)}$ = f20e533a + 27ccb387 = 19db06c1.

O resumo de mensagem de 256 bits resultante é

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

B.3 Exemplo de SHA-256 (mensagem longa)

Seja a mensagem *M* a forma codificada em binário da string ASCII que consiste em 1.000.000 de repetições do caractere “a”. O resumo da mensagem SHA-256 resultante é

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

APÊNDICE C: EXEMPLOS DE SHA-512

Este apêndice é apenas para fins informativos e não é necessário para atender ao padrão.

C.1 Exemplo de SHA-512 (mensagem de um bloco)

Deixe a mensagem, M, ser a string ASCII de 24 bits (l = 24) **"abc** ", que é equivalente à seguinte string binária:

01100001 01100010 01100011.

A mensagem é preenchida anexando um bit "1", seguido por 871 bits "0" e terminando com o valor hexadecimal

0000000000000000 00000000000000018

(as duas representações de palavra de 64 bits do comprimento, 24). Assim, a mensagem preenchida final consiste em um bloco *(N* = 1).

Para SHA-512, o valor de hash inicial, H(0), é

$H_0^{(0)}$ = 6a09e667f3bcc908
$H1^{(0)}$ = bb67ae8584caa73b
$H2^{(0)}$ = 3c6ef372fe94f82b
$H_3^{(0)}$ = a54ff53a5f1d36f1
$H4^{(0)}$ = 510e527fade682d1
$H_5^{(0)}$ = 9b05688c2b3e6c1f
$H_6^{(0)}$ = 1f83d9abfb41bd6b
$H_7^{(0)}$ = 5be0cd19137e2179.

As palavras do bloco de mensagens preenchidas são então atribuídas às palavras W0,…,W15 da programação de mensagens:

W0 = 6162638000000000
W1 = 0000000000000000
W2 = 0000000000000000
W3 = 0000000000000000
W4 = 0000000000000000
W5 = 0000000000000000
W6 = 0000000000000000
W7 = 0000000000000000
W8 = 0000000000000000 W9 =
0000000000000000 W10 =
0000000000000000 W11 =
0000000000000000 W12 =
00000000000000 W13 =

0000000000000000S0000000000000000 W13 = 0000

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 79" descrito na Seção 6.3.2, etapa 4.

	a / e	***b*** / ***f***	***c*** / g	***d*** / ***h***
t = 0:	f6arceb8bcfcddf5 58cb02347ab51f91	6a09e667f3bcc908 510e527fade682d1	bb67ae8584caa73b 9b05688c2b3e6c1f	3c6ef372fe94f82b 1f83d9abfb41bd6b
t = 1:	1320f8c9fb872cc0 c3d4ebfd48650ffa	f6aceb8bcfcddf5 58cb02347ab51f91	6a09e667f3bcc908 510e527fade682d1	bb67ae8584caa73b 9b05688c2b3e6c1f
t = 2:	ebcffc07203d91f3 dfa9b239f2697812	1320f8c9fb872cc0 c3d4ebfd48650ffa	f6aceb8bcfcddf5 58cb02347ab51f91	6a09e667f3bcc908 510e527fade682d1
t = 3:	5a83cb3e80050e82 0b47b4bb1928990e	ebcffc07203d91f3 dfa9b239f2697812	1320f8c9fb872cc0 c3d4ebfd48650ffa	f6aceb8bcfcddf5 58cb02347ab51f91
t = 4:	b680953951604860 745 aca4a342ed2e2	5a83cb3e80050e82 0b47b4bb1928990e	ebcffc07203d91f3 dfa9b239f2697812	1320f8c9fb872cc0 c3d4ebfd48650ffa
t = 5:	af573b02403e89cd 96f60209b6dc35ba	b680953951604860 745 aca4a342ed2e2	5a83cb3e80050e82 0b47b4bb1928990e	ebcffc07203d91f3 dfa9b239f2697812
t = 6:	c4875b0c7abc076b 5a6c781f54dcc00c	af573b02403e89cd 96f60209b6dc35ba	b680953951604860 745 aca4a342ed2e2	5a83cb3e80050e82 0b47b4bb1928990e
t = 7:	8093d195e0054fa3 86f67263a0f0ec0a	c4875b0c7abc076b 5a6c781f54dcc00c	af573b02403e89cd 96f60209b6dc35ba	b680953951604860 745 aca4a342ed2e2
t = 8:	f1eca5544cb89225 d0403c398fc40002	8093d195e0054fa3 86f67263a0f0ec0a	c4875b0c7abc076b 5a6c781f54dcc00c	af573b02403e89cd 96f60209b6dc35ba
t = 9:	81782d4a5db48f03 00091f460be46c52	f1eca5544cb89225 d0403c398fc40002	8093d195e0054fa3 86f67263a0f0ec0a	c4875b0c7abc076b 5a6c781f54dcc00c
t = 10:	69854c4aa0f25b59 d375471bde1ba3f4	81782d4a5db48f03 00091f460be46c52	f1eca5544cb89225 d0403c398fc40002	8093d195e0054fa3 86f67263a0f0ec0a
t = 11:	db0a9963f80c2eaa 475975b91a7a462c	69854c4aa0f25b59 d375471bde1ba3f4	81782d4a5db48f03 00091f460be46c52	f1eca5544cb89225 d0403c398fc40002
t = 12:	5e41214388186c14 cdf3bff2883fc9d9	db0a9963f80c2eaa 475975b91a7a462c	69854c4aa0f25b59 d375471bde1ba3f4	81782d4a5db48f03 00091f460be46c52
t = 13:	44249631255d2ca0 860acf9effba6f61	5e41214388186c14 cdf3bff2883fc9d9	db0a9963f80c2eaa 475975b91a7a462c	69854c4aa0f25b59 d375471bde1ba3f4
t = 14:	fa967eed85a08028 874bfe5f6aae9f2f	44249631255d2ca0 860acf9effba6f61	5e41214388186c14 cdf3bff2883fc9d9	db0a9963f80c2eaa 475975b91a7a462c
t = 15:	0ae07c86b1181c75 a77b7c035dd4c161	fa967eed85a08028 874bfe5f6aae9f2f	44249631255d2ca0 860acf9effba6f61	5e41214388186c14 cdf3bff2883fc9d9
t = 16:	caf81a425d800537 2deecc6b39d64d78	0ae07c86b1181c75 a77b7c035dd4c161	fa967eed85a08028 874bfe5f6aae9f2f	44249631255d2ca0 860acf9effba6f61
t = 17:	4725be249ad19e6b f47e8353f8047455	caf81a425d800537 2deecc6b39d64d78	0ae07c86b1181c75 a77b7c035dd4c161	fa967eed85a08028 874bfe5f6aae9f2f
t = 18:	3c4b4104168e3edb 29695fd88d81dbd0	4725be249ad19e6b f47e8353f8047455	caf81a425d800537 2deecc6b39d64d78	0ae07c86b1181c75 a77b7c035dd4c161
t = 19:	9a3fb4d38ab6cf06 f14998dd5f70767e	3c4b4104168e3edb 29695fd88d81dbd0	4725be249ad19e6b f47e8353f8047455	caf81a425d800537 2deecc6b39d64d78

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

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

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

Isso completa o processamento do primeiro e único bloco de mensagem, M(1). O valor de hash final, H(1), é calculado para ser

$H_0^{(1)}$ = 6a09e667f3bcc908 + 73a54f399fa4b1b2 = ddaf35a193617aba

$H_1^{(1)}$ = bb67ae8584caa73b + 10d9c4c4295599f6 = cc417349ae204131

$H_2^{(1)}$ = 3c6ef372fe94f82b + d67806db8b148677 = 12e6fa4e89a97ea2

$H_3^{(1)}$ = a54ff53a5f1d36f1 + 654ef9abec389ca9 = 0a9eeee64b55d39a

$H_4^{(1)}$ = 510e527fade682d1 + d08446aa79693ed7 = 2192992a274fc1a8

$H_5^{(1)}$ = 9b05688c2b3e6c1f + 9bb4d39778c07f9e = 36ba3c23a3feebbd

$H_6^{(1)}$ = 1f83d9abfb41bd6b + 25c96a7768fb2aa3 = 454d4423643ce80e

$H_7^{(1)}$ = 5be0cd19137e2179 + ceb9fc3691ce8326 = 2a9ac94fa54ca49f.

O resumo de mensagem de 512 bits resultante é

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

C.2 Exemplo de SHA-512 (mensagem de vários blocos)

Deixe a mensagem, M, ser a string ASCII de 896 bits (l = 896)

"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn
hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu".

A mensagem é preenchida anexando um bit "1", seguido por 1023 bits "0" e terminando com o valor hexadecimal

0000000000000000 0000000000000380

(as duas representações de palavra de 64 bits do comprimento, 896). Assim, a mensagem preenchida final consiste em dois blocos *(N* = 2).

Para SHA-512, o valor de hash inicial, H(0), é

$H0^{(0)}$ = 6a09e667f3bcc908
$H1^{(0)}$ = bb67ae8584caa73b
$H2^{(0)}$ = 3c6ef372fe94f82b
$H3^{(0)}$ = a54ff53a5f1d36f1
$H4^{(0)}$ = 510e527fade682d1
$H5^{(0)}$ = 9b05688c2b3e6c1f
$H6^{(0)}$ = 1f83d9abfb41bd6b
$H7^{(0)}$ = 5be0cd19137e2179.

As palavras do bloco de mensagens preenchidas são então atribuídas às palavras W0,…,W15 da programação de mensagens:

W0 = 61626366465666768
W1 = 6263646566676869
W2 = 636465666768696a
W3 = 6465666768696a6b
W4 = 65666768696a6b6c
W5 = 666768696a6b6c6d
W6 = 6768696a6b6c6d6e
W7 = 68696a6b6c6d6e6f
W8 = 696a6b6c6d6e6f70 W9 = 6a6b6c6d6e6f7071 W10 = 6b6c6d6e6f707172 W11 = 6c6d6e6f70717273 W12 = 6d6e6f7071727374 W13 = 6e6f707172737475 W14 = 8000000000000000 W15 = 0000000000000000.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop “for t = 0 to 79” descrito na Seção 6.3.2, etapa 4.

	a		***c***	
	/		***/***	
	e	***b/ f***	g	***d/ h***
t = 0: f6ace9d2263455d	6a09e667f3bcc908	bb67ae8584caa73b	3c6ef372fe94f82b	
58cb0218e01b86f9	510e527fade682d1	9b05688c2b3e6c1f	1f83d9abfb41bd6b	
t = 1: 0b7056a534ae5f62	f6ace9d2263455d	6a09e667f3bcc908	bb67ae8584caa73b	
f8c7198fe39e4c8c	58cb0218e01b86f9	510e527fade682d1	9b05688c2b3e6c1f	
t = 2: 2ca82233760c9942	0b7056a534ae5f62	f6ace9d2263455d	6a09e667f3bcc908	
303eccccd65953de	f8c7198fe39e4c8c	58cb0218e01b86f9	510e527fade682d1	
t = 3: a023f17ce52cda7b	2ca82233760c9942	0b7056a534ae5f62	f6ace9d2263455d	
ffdee5eedcc9ca42	303 eccccd65953de	f8c7198fe39e4c8c	58cb0218e01b86f9	
t = 4: 8f0a67d9d591a1a7	a023f17ce52cda7b	2ca82233760c9942	0b7056a534ae5f62	
cb4cfbb166505f2f	ffdee5eedcc9ca42	303 eccccd65953de	f8c7198fe39e4c8c	
t = 5: b466267371acc493	8f0a67d9d591a1a7	a023f17ce52cda7b	2ca82233760c9942	
73d6c84c54d399ee	cb4cfbb166505f2f	ffdee5eedcc9ca42	303 eccccd65953de	
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 64b5ae5424598428	1d47a3268ff677ed 8407818e9b28cc12	cdb73772dc0248bf dc8049afa6acd502	05f3fba454e5de3d caed4b5fa322b984
t = 23: be50606778de14a6	af4e23eb622d0df4	1d47a3268ff677ed	cdb73772dc0248bf
	0a5d727cc92e7adb	64b5ae5424598428	8407818e9b28cc12	dc8049afa6acd502
t = 24: 821e44f6678ac478f367e596d0a038a5	be50606778de14a6 0a5d727cc92e7adb	af4e23eb622d0df4 64b5ae5424598428	1d47a3268ff677ed 8407818e9b28cc12
t = 25: 0c852b1359a77c18 6dec8a3396a80c3f	821e44f6678ac478 f367e596d0a038a5	be50606778de14a6 0a5d727cc92e7adb	af4e23eb622d0df4 64b5ae5424598428
t = 26: ebb574fad4b7a7e4	0c852b1359a77c18	821e44f6678ac478	be50606778de14a6
	a241e7efc1eb6ff9	6dec8a3396a80c3f	f367e596d0a038a5	0a5d727cc92e7adb
t = 27: a092821c3cdf08da c84e849917a7c08e	ebb574fad4b7a7e4 a241e7efc1eb6ff9	0c852b1359a77c18 6dec8a3396a80c3f	821e44f6678ac478 f367e596d0a038a5
t = 28: 82ba2e1a2df2a4f1 61845f6924789851	a092821c3cdf08da c84e849917a7c08e	ebb574fad4b7a7e4 a241e7efc1eb6ff9	0c852b1359a77c18 6dec8a3396a80c3f
t = 29: 1959ad991c63d06a	82ba2e1a2df2a4f1	a092821c3cdf08da	ebb574fad4b7a7e4
	231faf24910a891a	61845f6924789851	c84e849917a7c08e	a241e7efc1eb6ff9
t = 30: 9b32d4cacd9a625b 533066919d608799	1959ad991c63d06a 231faf24910a891a	82ba2e1a2df2a4f1 61845f6924789851	a092821c3cdf08da c84e849917a7c08e
t = 31: dc55339f4d841965	9b32d4cacd9a625b	1959ad991c63d06a	82ba2e1a2df2a4f1
	e2517f359998a58d	533066919d608799	231faf24910a891a	61845f6924789851
t = 32: fdebb1283b12514f b1989170a183c661	dc55339f4d841965 e2517f359998a58d	9b32d4cacd9a625b 533066919d608799	1959ad991c63d06a 231faf24910a891a
t = 33: b44c7975a83e3334 009ad175b8d588a4	fdebb1283b12514f b1989170a183c661	dc55339f4d841965 e2517f359998a58d	9b32d4cacd9a625b 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 0f57062401dc680b	824408631432e09b 5e696a9fda56d6bf	392893c22e75856a 7a7c9eb7bc813248	0bac61bfc53d18b7 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 d688101dfd24a148	08f151f4b8d0fa2e ec8b96fe402094cd	b80591f6fbfadcde 00f4407c0f37237e	922537abad1e95a1 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 046735513cdd14d3	ca61990b43297ffc 139aa55c51d9ee5f	890c2cd670c4aea3 dd13e4edeeff00e7	a71bf5bd64289948 e052bfb7a6945939
t = 46: 1f0720944dbeb6a4	7196e8fa538ba4bf	ca61990b43297ffc	890c2cd670c4aea3
a41eb7e5a27588e3	046735513cdd14d3	139aa55c51d9ee5f	dd13e4edeeff00e7
t = 47: d6d4f8608b8ab199 24b9c216f915da60	1f0720944dbeb6a4 a41eb7e5a27588e3	7196e8fa538ba4bf 046735513cdd14d3	ca61990b43297ffc 139aa55c51d9ee5f
t = 48: 88761eb67845978e 9fe22e39448d50ed	d6d4f8608b8ab199 24b9c216f915da60	1f0720944dbeb6a4 a41eb7e5a27588e3	7196e8fa538ba4bf 046735513cdd14d3
t = 49: 7d40e6be47d85702	88761eb67845978e	d6d4f8608b8ab199	1f0720944dbeb6a4
d9c900e01968c33e	9fe22e39448d50ed	24b9c216f915da60	a41eb7e5a27588e3
t = 50: 7d0d988df5768598 2ec2e522a7c7d12c	7d40e6be47d85702 d9c900e01968c33e	88761eb67845978e 9fe22e39448d50ed	d6d4f8608b8ab199 24b9c216f915da60
t = 51: 48a8b60575b37f31	7d0d988df5768598	7d40e6be47d85702	88761eb67845978e
7059f9bc8c88a373	2ec2e522a7c7d12c	d9c900e01968c33e	9fe22e39448d50ed
t = 52: 6bc425af294bbf79 6a8143b1716ee33d	48a8b60575b37f31 7059f9bc8c88a373	7d0d988df5768598 2ec2e522a7c7d12c	7d40e6be47d85702 d9c900e01968c33e
t = 53: 307a456158ee8849	6bc425af294bbf79	48a8b60575b37f31	7d0d988df5768598
4372e85c16ee4440	6a8143b1716ee33d	7059f9bc8c88a373	2ec2e522a7c7d12c
t = 54: af36382c8fd716be a8f8b0033187a916	307a456158ee8849 4372e85c16ee4440	6bc425af294bbf79 6a8143b1716ee33d	48a8b60575b37f31 7059f9bc8c88a373
t = 55: 810ebee951c64ca1 16a64f5997b9cca6	af36382c8fd716be a8f8b0033187a916	307a456158ee8849 4372e85c16ee4440	6bc425af294bbf79 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 9fc52468b897f9c8	c1af358833cb03c0 d4883c0c21dda190	5ac712acff4b98be 91f6395b301adbfd	2dd7659f1b4d13cd 5da6793bb7286a4b
t = 60: f11bfd0cf67d3040 47efb6407f74d318	88a306074d388c7d 9fc52468b897f9c8	c1af358833cb03c0 d4883c0c21dda190	5ac712acff4b98be 91f6395b301adbfd
t = 61: 1f065e7828ed4e1b 7481899904a4ce23	f11bfd0cf67d3040 47efb6407f74d318	88a306074d388c7d 9fc52468b897f9c8	c1af358833cb03c0 d4883c0c21dda190
t = 62: aebde39f2bc42ec1	1f065e7828ed4e1b	f11bfd0cf67d3040	88a306074d388c7d
62ab526ff177a988	7481899904a4ce23	47efb6407f74d318	9fc52468b897f9c8
t = 63: d35a94706e3e5df2 53f92b648d5d815c	aebde39f2bc42ec1 62ab526ff177a988	1f065e7828ed4e1b 7481899904a4ce23	f11bfd0cf67d3040 47efb6407f74d318
t = 64: d72d727c53e09ab9	d35a94706e3e5df2	aebde39f2bc42ec1	1f065e7828ed4e1b
10746426ba9824f4	53f92b648d5d815c	62ab526ff177a988	7481899904a4ce23
t = 65: 3a7235e5a4051d94 afe455daec5c2b00	d72d727c53e09ab9 10746426ba9824f4	d35a94706e3e5df2 53f92b648d5d815c	aebde39f2bc42ec1 62ab526ff177a988
t = 66: f7f510fe73ef7e76 f1202c0bb7c4583f	3a7235e5a4051d94 afe455daec5c2b00	d72d727c53e09ab9 10746426ba9824f4	d35a94706e3e5df2 53f92b648d5d815c
t = 67: 23c2acfb393523e9	f7f510fe73ef7e76	3a7235e5a4051d94	d72d727c53e09ab9
a0bc2a61044ac12e	f1202c0bb7c4583f	afe455daec5c2b00	10746426ba9824f4

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

Isso completa o processamento do primeiro bloco de mensagem, M(1). O valor de hash intermediário, H(1), é calculado para ser

$H_0^{(1)}$ = 6a09e667f3bcc908 + d90f1b1237b3a561 = 4319017a2b706e69

$H_1^{(1)}$ = bb67ae8584caa73b + 11e3570e06e3b74e = cd4b05938bae5e89

$H_2^{(1)}$ = 3c6ef372fe94f82b + c517cba6a09bb26a = 0186bf199f30aa95

$H_3^{(1)}$ = a54ff53a5f1d36f1 + c9a8c1e2d063ce94 = 6ef8b71d2f810585

$H_4^{(1)}$ = 510e527fade682d1 + 867983f69d3a3ad1 = d787d6764b20bda2

$H_5^{(1)}$ = 9b05688c2b3e6c1f + 075aabbade34fd01 = a260144709736920

$H_6^{(1)}$ = 1f83d9abfb41bd6b + e1682bd33c8f8e23 = 00ec057f37d14b8e

$H_7^{(1)}$ = 5be0cd19137e2179 + aacd089bfae8faf9 = 06add5b50e671c72.

As palavras do *segundo* bloco de mensagem acolchoado, M(2), são então atribuídas às palavras W0,…,W15 da programação de mensagem:

W0 = 00000000000000000 W8 = 0000000000000000 W9 =
W1 = 00000000000000000 0000000000000000 W10 =
W2 = 00000000000000000 0000000000000000 W11 =
W3 = 00000000000000000 0000000000000000 W12 =
W4 = 00000000000000000 00000000000000 W13 =
W5 = 00000000000000000
W6 = 0000000000000000
W7 = 00000000000000000 00000000000000000S0000000000000000 W13 = 00000

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 79" descrito na Seção 6.1.2, etapa 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 1b6d7234ace15d7d	f8e6924412fd0c64 d50cf4f73910e3ee	c1700e250dc6ffed 970088839126bda5	1ce4f2591812e6ae b27252537a83cf27
t = 63: 3960545ab926c0d5 9eabb5618b4fcd13	d53e0a39eee47528 1b6d7234ace15d7d	f8e6924412fd0c64 d50cf4f73910e3ee	c1700e250dc6ffed 970088839126bda5
t = 64: b2c164d71abb92fe f1736fbbfb6ebe72	3960545ab926c0d5 9eabb5618b4fcd13	d53e0a39eee47528 1b6d7234ace15d7d	f8e6924412fd0c64 d50cf4f73910e3ee
t = 65: 4d979e985b067e75 d1fb300f35992350	b2c164d71abb92fe f1736fbbfb6ebe72	3960545ab926c0d5 9eabb5618b4fcd13	d53e0a39eee47528 1b6d7234ace15d7d
t =66: 59d0238ce137abd7 5f3c64b7546e2cec	4d979e985b067e75 d1fb300f35992350	b2c164d71abb92fe f1736fbbfb6ebe72	3960545ab926c0d5 9eabb5618b4fcd13
t = 67: bf8d9453b9876b0a 6c27893a31b0e07e	59d0238ce137abd7 5f3c64b7546e2cec	4d979e985b067e75 d1fb300f35992350	b2c164d71abb92fe f1736fbbfb6ebe72
t = 68: c45dd4a2d2fea059 48253e21b26d8cf9	bf8d9453b9876b0a 6c27893a31b0e07e	59d0238ce137abd7 5f3c64b7546e2cec	4d979e985b067e75 d1fb300f35992350
t = 69: e08471946c17b0b6 714e2adf4e23ff24	c45dd4a2d2fea059 48253e21b26d8cf9	bf8d9453b9876b0a 6c27893a31b0e07e	59d0238ce137abd7 5f3c64b7546e2cec
t = 70: b4838c1c28fee7bc 371f12f333f7e5b9	e08471946c17b0b6 714e2adf4e23ff24	c45dd4a2d2fea059 48253e21b26d8cf9	bf8d9453b9876b0a 6c27893a31b0e07e
t = 71: 851cf60a77f6e6d1 a2a475deac0e8b42	b4838c1c28fee7bc 371f12f333f7e5b9	e08471946c17b0b6 714e2adf4e23ff24	c45dd4a2d2fea059 48253e21b26d8cf9
t = 72: f53d23c50249af2d 1e99cae9d4cf0409	851cf60a77f6e6d1 a2a475deac0e8b42	b4838c1c28fee7bc 371f12f333f7e5b9	e08471946c17b0b6 714e2adf4e23ff24
t = 73: b81e85d427045550 f5794711faa60f63	f53d23c50249af2d 1e99cae9d4cf0409	851cf60a77f6e6d1 a2a475deac0e8b42	b4838c1c28fee7bc 371f12f333f7e5b9
t = 74: ae70c7d11ea84a83 dc0d633411c289b2	b81e85d427045550 f5794711faa60f63	f53d23c50249af2d 1e99cae9d4cf0409	851cf60a77f6e6d1 a2a475deac0e8b42
t = 75: 5c54592e13c76135 1620dd5479e94b9b	ae70c7d11ea84a83 dc0d633411c289b2	b81e85d427045550 f5794711faa60f63	f53d23c50249af2d 1e99cae9d4cf0409
t =76: 03a0f79087078a93 57e90fa678e4cc97	5c54592e13c76135 1620dd5479e94b9b	ae70c7d11ea84a83 dc0d633411c289b2	b81e85d427045550 f5794711faa60f63
t = 77: 8df0baad4c6ed50c c6e7246f7f0bdac6	03a0f79087078a93 57e90fa678e4cc97	5c54592e13c76135 1620dd5479e94b9b	ae70c7d11ea84a83 dc0d633411c289b2
t = 78: bfa9f194894db5b6 90bb8597bb41da1a	8df0baad4c6ed50c c6e7246f7f0bdac6	03a0f79087078a93 57e90fa678e4cc97	5c54592e13c76135 1620dd5479e94b9b
t = 79: 4b7c99fbaf72a571 78955227fde03a42	bfa9f194894db5b6 90bb8597bb41da1a	8df0baad4c6ed50c c6e7246f7f0bdac6	03a0f79087078a93 57e90fa678e4cc97

Isso completa o processamento do segundo e último bloco de mensagem, M(2). O valor de hash final, H(2), é calculado para ser

$H_0^{(2)}$ = 4319017a2b706e69 + 4b7c99fbaf72a571 = 8e959b75dae313da

$H1^{(2)}$ = cd4b05938bae5e89 + bfa9f194894db5b6 = 8cf4f72814fc143f

$H2^{(2)}$ = 0186bf199f30aa95 + 8df0baad4c6ed50c = 8f7779c6eb9f7fa1

$H_3^{(2)}$ = 6ef8b71d2f810585 + 03a0f79087078a93 = 7299aadb6889018

$H4^{(2)}$ = d787d6764b20bda2 + 78955227fde03a42 = 501d289e4900f7e4

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

$H_6^{(2)}$ = 00ec057f37d14b8e + c6e7246f7f0bdac6 = c7d329eb6dd2654

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

O resumo de mensagem de 512 bits resultante é

8e959b75dae313da 8cf4f72814fc143f 8f7779c6eb9f7fa1 7299aeadb6889018

501d289e4900f7e4 331b99dec4b5433a c7d329eb6dd2654 5e96e55b874be909.

C.3 Exemplo de SHA-512 (mensagem longa)

Seja a mensagem *M* a forma codificada em binário da string ASCII que consiste em 1.000.000 de repetições do caractere “a”.
O resumo da mensagem SHA-512 resultante é

e718483d0ce76964 4e2e42c7bc15b463 8e1f98b13b204428 5632a803afa973eb

de0ff244877ea60a 4cb0432ce577c31b eb009c5c2c49aa2e 4eadb217ad8cc09b.

APÊNDICE D: EXEMPLOS SHA-384

Este apêndice é apenas para fins informativos e não é necessário para atender ao padrão.

D.1 Exemplo SHA-384 (mensagem de um bloco)

Deixe a mensagem, M, ser a string ASCII de 24 bits (l = 24) **"abc** ", que é equivalente à seguinte string binária:

01100001 01100010 01100011.

A mensagem é preenchida anexando um bit "1", seguido por 871 bits "0" e terminando com o valor hexadecimal

0000000000000000 00000000000000018

(as duas representações de palavra de 64 bits do comprimento, 24). Assim, a mensagem preenchida final consiste em um bloco *(N* = 1).

Para SHA-384, o valor de hash inicial, H(0), é

$H_0^{(0)}$ = cbbb9d5dc1059ed8
$H1^{(0)}$ = 629a292a367cd507
$H2^{(0)}$ = 9159015a3070dd17
$H_3^{(0)}$ = 152fecd8f70e5939
$H4^{(0)}$ = 67332667ffc00b31
$H_5^{(0)}$ = 8eb44a8768581511
$H_6^{(0)}$ = db0c2e0d64f98fa7
$H_7^{(0)}$ = 47b5481dbefa4fa4.

As palavras do bloco de mensagens preenchidas são então atribuídas às palavras W0,…,W15 da programação de mensagens:

W0 = 6162638000000000
W1 = 0000000000000000
W2 = 0000000000000000
W3 = 0000000000000000
W4 = 0000000000000000
W5 = 0000000000000000
W6 = 0000000000000000
W7 = 0000000000000000
W8 = 0000000000000000 W9 = 0000000000000000 W10 = 0000000000000000 W11 = 0000000000000000 W12 = 00000000000000 W13 =

0000000000000000S0000000000000000 W13 = 0000

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 79" descrito na Seção 6.3.2, etapa 4.

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

t = 20: 9ba737ae88a72c64 3fc2614c43906c0f	f1aabd313309509b 674385f0d87db94f	63a24014a34bb0f6 e13e610eae680d85	7df1b65f1b87d6ca 5b6e369d36e8e181
t = 21: 042c2dc9a5bf558a 19316bebc88e01f2	9ba737ae88a72c64 3fc2614c43906c0f	f1aabd313309509b 674385f0d87db94f	63a24014a34bb0f6 e13e610eae680d85
t = 22: 7799c75acc748c0f a7bbd65bf64f58c8	042c2dc9a5bf558a 19316bebc88e01f2	9ba737ae88a72c64 3fc2614c43906c0f	f1aabd313309509b 674385f0d87db94f
t = 23: ccf99a80f92bf002 e52a24fae4e8fc9b	7799c75ac748c0f a7bbd65bf64f58c8	042c2dc9a5bf558a 19316bebc88e01f2	9ba737ae88a72c64 3fc2614c43906c0f
t = 24: ae993474363efe68 587f308d58681928	ccf99a80f92bf002 e52a24fae4e8fc9b	7799c75ac748c0f a7bbd65bf64f58c8	042c2dc9a5bf558a 19316bebc88e01f2
t = 25: 335063d1a2aec92f c2d6d65e38c6ea79	ae993474363efe68 587f308d58681928	ccf99a80f92bf002 e52a24fae4e8fc9b	7799c75ac748c0f a7bbd65bf64f58c8
t =26: 53a78b0cca01ba37 3b65a26c3c92c8f3	335063d1a2aec92f c2d6d65e38c6ea79	ae993474363efe68 587f308d58681928	ccf99a80f92bf002 e52a24fae4e8fc9b
t = 27: ab7ffa529f622930 b9d8a2f2762901ea	53a78b0cca01ba37 3b65a26c3c92c8f3	335063d1a2aec92f c2d6d65e38c6ea79	ae993474363efe68 587f308d58681928
t =28: e428bb43afe3d63e 6a8527525f898726	ab7ffa529f622930 b9d8a2f2762901ea	53a78b0cca01ba37 3b65a26c3c92c8f3	335063d1a2aec92f c2d6d65e38c6ea79
t = 29: bbed541a5128088c 7973aadbde294be9	e428bb43afe3d63e 6a8527525f898726	ab7ffa529f622930 b9d8a2f2762901ea	53a78b0cca01ba37 3b65a26c3c92c8f3
t = 30: 4c5c38df7ec8baf4 422ceea0200e9ee4	bbed541a5128088c 7973aadbde294be9	e428bb43afe3d63e 6a8527525f898726	ab7ffa529f622930 b9d8a2f2762901ea
t = 31: 4ba456ec244033ed 7cf40857056d86b0	4c5c38df7ec8baf4 422ceea0200e9ee4	bbed541a5128088c 7973aadbde294be9	e428bb43afe3d63e 6a8527525f898726
t = 32: aa4a6ab2ac5f5dd8 ad2b1ecfb5bfc556	4ba456ec244033ed 7cf40857056d86b0	4c5c38df7ec8baf4 422ceea0200e9ee4	bbed541a5128088c 7973aadbde294be9
t = 33: 9cb941f2ced774b3 029f66c7b4569bf0	aa4a6ab2ac5f5dd8 ad2b1ecfb5bfc556	4ba456ec244033ed 7cf40857056d86b0	4c5c38df7ec8baf4 422ceea0200e9ee4
t = 34: 39265f358594de27 3f7b1c260c82e54f	9cb941f2ced774b3 029f66c7b4569bf0	aa4a6ab2ac5f5dd8 ad2b1ecfb5bfc556	4ba456ec244033ed 7cf40857056d86b0
t = 35: 09cca487d39b02a1 4a22b37b58a5b1b0	39265f358594de27 3f7b1c260c82e54f	9cb941f2ced774b3 029f66c7b4569bf0	aa4a6ab2ac5f5dd8 ad2b1ecfb5bfc556
t = 36: d48d97ce438cf4f0 a239e00b8baa0410	09cca487d39b02a1 4a22b37b58a5b1b0	39265f358594de27 3f7b1c260c82e54f	9cb941f2ced774b3 029f66c7b4569bf0
t = 37: d6f41e25a8b634d6 25755cb8179dd0b0	d48d97ce438cf4f0 a239e00b8baa0410	09cca487d39b02a1 4a22b37b58a5b1b0	39265f358594de27 3f7b1c260c82e54f
t = 38: 54078334358573b4 0e419fb0802b0efc	d6f41e25a8b634d6 25755cb8179dd0b0	d48d97ce438cf4f0 a239e00b8baa0410	09cca487d39b02a1 4a22b37b58a5b1b0
t = 39: db24f9a03f4fff6b d30e99b4b394b090	54078334358573b4 0e419fb0802b0efc	d6f41e25a8b634d6 25755cb8179dd0b0	d48d97ce438cf4f0 a239e00b8baa0410
t = 40: 3604c53a845efc37 791b2b4af7338b99	db24f9a03f4fff6b d30e99b4b394b090	54078334358573b4 0e419fb0802b0efc	d6f41e25a8b634d6 25755cb8179dd0b0
t = 41: f41b1c0eee89bdc6 e319b77d9e4e87f9	3604c53a845efc37 791b2b4af7338b99	db24f9a03f4fff6b d30e99b4b394b090	54078334358573b4 0e419fb0802b0efc
t = 42: 36644ae374632e3a 458250878a3972b2	f41b1c0eee89bdc6 e319b77d9e4e87f9	3604c53a845efc37 791b2b4af7338b99	db24f9a03f4fff6b d30e99b4b394b090
t = 43: 88806f6ae9fcd65b	36644ae374632e3a	f41b1c0eee89bdc6	3604c53a845efc37

cfde2e6ea54fa576	458250878a3972b2	e319b77d9e4e87f9	791b2b4af7338b99
t = 44: 51dcaa36995c301d e37f778353998050	88806f6ae9fcd65b cfde2e6ea54fa576	36644ae374632e3a 458250878a3972b2	f41b1c0eee89bdc6 e319b77d9e4e87f9
t = 45: ef5e3885a2f238df 740e347f24e18fda	51dcaa36995c301d e37f778353998050	88806f6ae9fcd65b cfde2e6ea54fa576	36644ae374632e3a 458250878a3972b2
t = 46: eb3753f4283f4818 0ae48cf840bb8be9	ef5e3885a2f238df 740e347f24e18fda	51dcaa36995c301d e37f778353998050	88806f6ae9fcd65b cfde2e6ea54fa576
t = 47: a6998d63a5d09e04 e21095012ee0b72a	eb3753f4283f4818 0ae48cf840bb8be9	ef5e3885a2f238df 740e347f24e18fda	51dcaa36995c301d e37f778353998050
t = 48: d3698fb64df175b0 c2f0b90fce80739	a6998d63a5d09e04 e21095012ee0b72a	eb3753f4283f4818 0ae48cf840bb8be9	ef5e3885a2f238df 740e347f24e18fda
t = 49: 317a3b295b991914 1cadff2e6cb5aa4d	d3698fb64df175b0 c2f0b90fce80739	a6998d63a5d09e04 e21095012ee0b72a	eb3753f4283f4818 0ae48cf840bb8be9
t = 50: 0941da08148ba463 833eb9a4bb5a073e	317a3b295b991914 1cadff2e6cb5aa4d	d3698fb64df175b0 c2f0b90fce80739	a6998d63a5d09e04 e21095012ee0b72a
t = 51: 494ac238d68c3d0b 80c8fc138e645028	0941da08148ba463 833eb9a4bb5a073e	317a3b295b991914 1cadff2e6cb5aa4d	d3698fb64df175b0 c2f0b90fce80739
t = 52: c87e9168db9e97de 65cf7f6a829aca04	494ac238d68c3d0b 80c8fc138e645028	0941da08148ba463 833eb9a4bb5a073e	317a3b295b991914 1cadff2e6cb5aa4d
t = 53: edb4448879391dbb 7729c85475dd318f	c87e9168db9e97de 65cf7f6a829aca04	494ac238d68c3d0b 80c8fc138e645028	0941da08148ba463 833eb9a4bb5a073e
t = 54: 073775c2456dc7db a9cca0b6266b1d77	edb4448879391dbb 7729c85475dd318f	c87e9168db9e97de 65cf7f6a829aca04	494ac238d68c3d0b 80c8fc138e645028
t = 55: 54de8857b24afaf7 8de51cff2ae4b068	073775c2456dc7db a9cca0b6266b1d77	edb4448879391dbb 7729c85475dd318f	c87e9168db9e97de 65cf7f6a829aca04
t = 56: 8a9cdd80f7f09c05 a60ba5e9ebaeb96a	54de8857b24afaf7 8de51cff2ae4b068	073775c2456dc7db a9cca0b6266b1d77	edb4448879391dbb 7729c85475dd318f
t = 57: 3eeb22a7524d8d7f e2e6830b139df58f	8a9cdd80f7f09c05 a60ba5e9ebaeb96a	54de8857b24afaf7 8de51cff2ae4b068	073775c2456dc7db a9cca0b6266b1d77
t =58: 0ed77c9cde8883d3 38413a2052387a9e	3eeb22a7524d8d7f e2e6830b139df58f	8a9cdd80f7f09c05 a60ba5e9ebaeb96a	54de8857b24afaf7 8de51cff2ae4b068
t = 59: e64e4135f9d30dbc 45b640454c75c349	0ed77c9cde8883d3 38413a2052387a9e	3eeb22a7524d8d7f e2e6830b139df58f	8a9cdd80f7f09c05 a60ba5e9ebaeb96a
t = 60: 1ca93a293d544328 efbef83a35c0319e	e64e4135f9d30dbc 45b640454c75c349	0ed77c9cde8883d3 38413a2052387a9e	3eeb22a7524d8d7f e2e6830b139df58f
t = 61: 3dc764f89e54043a a57784945550cf94	1ca93a293d544328 efbef83a35c0319e	e64e4135f9d30dbc 45b640454c75c349	0ed77c9cde8883d3 38413a2052387a9e
t = 62: 56fb5883f1c87a05 f5198a41eb80e022	3dc764f89e54043a a57784945550cf94	1ca93a293d544328 efbef83a35c0319e	e64e4135f9d30dbc 45b640454c75c349
t = 63: 24a1124262a331c7 06edacae6e7b54ad	56fb5883f1c87a05 f5198a41eb80e022	3dc764f89e54043a a57784945550cf94	1ca93a293d544328 efbef83a35c0319e
t = 64: eb85d19201c89694 9ced24983eec8723	24a1124262a331c7 06edacae6e7b54ad	56fb5883f1c87a05 f5198a41eb80e022	3dc764f89e54043a a57784945550cf94
t = 65: cc981ab3a59c1db4 eac5516336bc8882	eb85d19201c89694 9ced24983eec8723	24a1124262a331c7 06edacae6e7b54ad	56fb5883f1c87a05 f5198a41eb80e022
t = 66: ceef5d997e148b44 617bbf70bb165212	cc981ab3a59c1db4 eac5516336bc8882	eb85d19201c89694 9ced24983eec8723	24a1124262a331c7 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	8c5d3b7fpai66e70	1e6e0255ab88079f	689edf608a8e3f14
51105f6241313777	90d18ec8b69f0345	f2001138439902b1	3280d88472c100fd
t = 71: bcd5061679be7336	32e5ed8655871e9b	8c5d3b7fpai66e70	1e6e0255ab88079f
454b99f654443ad0	51105f6241313777	90d18ec8b69f0345	f2001138439902b1
t = 72: e7d913b6678e78ef	bcd5061679be7336	32e5ed8655871e9b	8c5d3b7fpai66e70
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

Isso completa o processamento do primeiro e único bloco de mensagem, M(1). O valor de hash final, H(1), é calculado para ser

$H_0^{(1)}$ = cbbb9d5dc1059ed8 + ff44d7e1849dbfb3 = cb00753f45a35e8b

$H_1^{(1)}$ = 629a292a367cd507 + 5306143f64497b00 = b5a03d699ac65007

$H_2^{(1)}$ = 9159015a3070dd17 + 95d33150de6df44c = 272c32ab0eded163

$H_3^{(1)}$ = 152fecd8f70e5939 + 055b73814cf102b4 = 1a8b605a43ff5bed

$H_4^{(1)}$ = 67332667ffc00b31 + 1952e0c3a227c0f2 = 8086072ba1e7cc23

$H_5^{(1)}$ = 8eb44a8768581511 + ca06a219cc701096 = 58baeca134c825a7

$H_6^{(1)}$ = db0c2e0d64f98fa7 + c7f7bff08ebf0d30 = a303edfdf3b89cd7

$H_7^{(1)}$ = 47b5481dbefa4fa4 + c4b149710f5d6a71 = 0c66918ece57ba15.

O valor de hash final é truncado para seus 384 bits mais à esquerda (ou seja, $H_0^{(1)}$,K, $H_5^{(1)}$), resultando em 384 bits resumo da mensagem

cb00753f45a35e8b b5a03d699ac65007 272c32ab0eded163 1a8b605a43ff5bed

8086072ba1e7cc23 58baeca134c825a7.

D.2 Exemplo de SHA-384 (mensagem de vários blocos)

Deixe a mensagem, M, ser a string ASCII de 896 bits (l = 896)

"abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmn hijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu".

A mensagem é preenchida anexando um bit "1", seguido por 1023 bits "0" e terminando com o valor hexadecimal

0000000000000000 00000000000000380

(as duas representações de palavra de 64 bits do comprimento, 896). Assim, a mensagem preenchida final consiste em dois blocos *(N* = 2).

Para SHA-384, o valor de hash inicial, H(0), é

$H0^{(0)}$ = cbbb9d5dc1059ed8
$H1^{(0)}$ = 629a292a367cd507
$H2^{(0)}$ = 9159015a3070dd17
$H3^{(0)}$ = 152fecd8f70e5939
$H4^{(0)}$ = 67332667ffc00b31
$H5^{(0)}$ = 8eb44a8768581511
$H6^{(0)}$ = db0c2e0d64f98fa7
$H7^{(0)}$ = 47b5481dbefa4fa4.

As palavras do bloco de mensagens preenchidas são então atribuídas às palavras W0,…,W15 da programação de mensagens:

W0 = 61626366465666768
W1 = 6263646566676869
W2 = 636465666768696a
W3 = 6465666768696a6b
W4 = 65666768696a6b6c
W5 = 666768696a6b6c6d
W6 = 6768696a6b6c6d6e
W7 = 68696a6b6c6d6e6f
W8 = 696a6b6c6d6e6f70 W9 = 6a6b6c6d6e6f7071 W10 = 6b6c6d6e6f707172 W11 = 6c6d6e6f70717273 W12 = 6d6e6f7071727374 W13 = 6e6f707172737475 W14 = 8000000000000000 W15 = 0000000000000000.

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop “for t = 0 to 79” descrito na Seção 6.3.2, etapa 4.

	a		***c***	
	/		***/***	
	e	***b/ f***	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	69397 de9a30e1473	21af3c6430a9af9c	dd371f2d13661c52	
t = 8: 0f79040546e6edf7	412db7f990563d7c	b352d03a0bd34d65	27aaafb7fbef806b	
6b6c511b25a6bdbc	5062fd5924e2b62e	69397 de9a30e1473	21af3c6430a9af9c	
t = 9: ebf02410f67b8ee7	0f79040546e6edf7	412db7f990563d7c	b352d03a0bd34d65	
dac695b91543ae80	6b6c511b25a6bdbc	5062fd5924e2b62e	69397 de9a30e1473	
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 d49cef5bd2dec121	29c5348d87cd5590 4324c8caccf7753c	5eab10b19a5143a8 98d2b19d201f2bb6	f2911c11c96e5ff5 1bc2160f4f3711dc
t = 23: 1db4ee606d2a7a96 b17d15b397521ab3	33c6b4a0166b7c9c d49cef5bd2dec121	29c5348d87cd5590 4324c8caccf7753c	5eab10b19a5143a8 98d2b19d201f2bb6
t = 24: 5cef5b2f00142660 789e540f22e13932	1db4ee606d2a7a96 b17d15b397521ab3	33c6b4a0166b7c9c d49cef5bd2dec121	29c5348d87cd5590 4324c8caccf7753c
t = 25: ff74f4a162435903 6c0be33dcc6e7572	5cef5b2f00142660 789e540f22e13932	1db4ee606d2a7a96 b17d15b397521ab3	33c6b4a0166b7c9c d49cef5bd2dec121
t = 26: 41740b736e9676a9 d8e401251592da6c	ff74f4a162435903 6c0be33dcc6e7572	5cef5b2f00142660 789e540f22e13932	1db4ee606d2a7a96 b17d15b397521ab3
t = 27: 931059fe9279ff1d 7f31116887eea596	41740b736e9676a9 d8e401251592da6c	ff74f4a162435903 6c0be33dcc6e7572	5cef5b2f00142660 789e540f22e13932
t = 28: 356d08d982e2ead4 40c28c34b1bbe906	931059fe9279ff1d 7f31116887eea596	41740b736e9676a9 d8e401251592da6c	ff74f4a162435903 6c0be33dcc6e7572
t = 29: 89dc825e7235c74b 7a499ae05da50bf2	356d08d982e2ead4 40c28c34b1bbe906	931059fe9279ff1d 7f31116887eea596	41740b736e9676a9 d8e401251592da6c
t = 30: 97901f333e662fdc 4472b2e331ddfab4	89dc825e7235c74b 7a499ae05da50bf2	356d08d982e2ead4 40c28c34b1bbe906	931059fe9279ff1d 7f31116887eea596
t = 31: 69c8f40eb38b6022 177589502dd39aa2	97901f333e662fdc 4472b2e331ddfab4	89dc825e7235c74b 7a499ae05da50bf2	356d08d982e2ead4 40c28c34b1bbe906
t = 32: 4920943ffe52b207 6b813a0d0cdf4991	69c8f40eb38b6022 177589502dd39aa2	97901f333e662fdc 4472b2e331ddfab4	89dc825e7235c74b 7a499ae05da50bf2
t = 33: b4cb0df332d108ab 8fe3d28097f18618	4920943ffe52b207 6b813a0d0cdf4991	69c8f40eb38b6022 177589502dd39aa2	97901f333e662fdc 4472b2e331ddfab4
t = 34: e7748fbf744a5240 0d7ab03208f1d7a5	b4cb0df332d108ab 8fe3d28097f18618	4920943ffe52b207 6b813a0d0cdf4991	69c8f40eb38b6022 177589502dd39aa2
t = 35: 7416ca18d9e265e0 11200c2d47c082f8	e7748fbf744a5240 0d7ab03208f1d7a5	b4cb0df332d108ab 8fe3d28097f18618	4920943ffe52b207 6b813a0d0cdf4991
t = 36: 75476f5456e82f9c 3024702447f76224	7416ca18d9e265e0 11200c2d47c082f8	e7748fbf744a5240 0d7ab03208f1d7a5	b4cb0df332d108ab 8fe3d28097f18618
t = 37: f638a568b53a2f8f 6217c1c02153302c	75476f5456e82f9c 3024702447f76224	7416ca18d9e265e0 11200c2d47c082f8	e7748fbf744a5240 0d7ab03208f1d7a5
t = 38: c418f6f90602c79a 87f0901c227adbb3	f638a568b53a2f8f 6217c1c02153302c	75476f5456e82f9c 3024702447f76224	7416ca18d9e265e0 11200c2d47c082f8
t = 39: 4f1f4f21df3dcf43 fb7c63fcddf4a1c2	c418f6f90602c79a 87f0901c227adbb3	f638a568b53a2f8f 6217c1c02153302c	75476f5456e82f9c 3024702447f76224
t = 40: 13eb82e4b98d0e67 fb6c0e54d48d4f2d	4f1f4f21df3dcf43 fb7c63fcddf4a1c2	c418f6f90602c79a 87f0901c227adbb3	f638a568b53a2f8f 6217c1c02153302c
t = 41: 820e75046567bace b16a9397472f0123	13eb82e4b98d0e67 fb6c0e54d48d4f2d	4f1f4f21df3dcf43 fb7c63fcddf4a1c2	c418f6f90602c79a 87f0901c227adbb3
t = 42: 741fa5dc290dd02c ed40c88214823792	820e75046567bace b16a9397472f0123	13eb82e4b98d0e67 fb6c0e54d48d4f2d	4f1f4f21df3dcf43 fb7c63fcddf4a1c2
t = 43: a4809bf6da6aa8bd bec3d7e88c855194	741fa5dc290dd02c ed40c88214823792	820e75046567bace b16a9397472f0123	13eb82e4b98d0e67 fb6c0e54d48d4f2d
t = 44: d70b1aa4c800979c	a4809bf6da6aa8bd	741fa5dc290dd02c	820e75046567bace

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

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

Isso completa o processamento do primeiro bloco de mensagem, M(1). O valor de hash intermediário, H(1), é calculado para ser

$H_0^{(1)}$ = cbbb9d5dc1059ed8 + 5ec3802b9ecfef33 = 2a7f1d895fd58e0b

$H_1^{(1)}$ = 629a292a367cd507 + 88146da76ff6f23a = eaae96d1a673c741

$H_2^{(1)}$ = 9159015a3070dd17 + 7001201948fb3d71 = 015a2173796c1a88

$H_3^{(1)}$ = 152fecd8f70e5939 + e1053fc85f9e56be = f6352ca156acaff7

$H_4^{(1)}$ = 67332667ffc00b31 + 5f2eead69efb4233 = c662113e9ebb4d64

$H_5^{(1)}$ = 8eb44a8768581511 + 8901cffe7a74db98 = 17b61a85e2ccf0a9

$H_6^{(1)}$ = db0c2e0d64f98fa7 + 5cdf6c58fc052572 = 37eb9a6660feb519

$H_7^{(1)}$ = 47b5481dbefa4fa4 + 4779767cc2ec5321 = 8f2ebe9a81e6a2c5.

As palavras do *segundo* bloco de mensagem acolchoado, M(2), são então atribuídas às palavras W0,…,W15 da programação de mensagem:

W0 = 00000000000000000 W8 = 0000000000000000 W9 =
W1 = 00000000000000000 0000000000000000 W10 =
W2 = 00000000000000000 0000000000000000 W11 =
W3 = 00000000000000000 0000000000000000 W12 =
W4 = 00000000000000000 00000000000000 W13 =
W5 = 00000000000000000
W6 = 0000000000000000
W7 = 00000000000000000 00000000000000000S0000000000000000 W13 = 00000

A tabela a seguir mostra os valores hexadecimais para a, b, c, d, e, f, g e ***h*** *após* a passagem *t* do loop "for t = 0 to 79" descrito na Seção 6.3.2, etapa 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: 24c84b58d119afe	f1bd2d46be619585	9bc3871be8046113	f8a6b3fe2e4f0634
5ae0b1175beb5d2b	e47b9933bafdc655	05542ecd9883c6ba	602663c0f34eff33
t = 38: ec6d3abc2b291fd3	24c84b58d119affe	f1bd2d46be619585	9bc3871be8046113

	9ecc381d277748a3	5ae0b1175beb5d2b	e47b9933bafdc655	05542ecd9883c6ba
t = 39: e266c1f77d5ee90e d92f34c110296b32	ec6d3abc2b291fd3 9ecc381d277748a3	24c84b58d119affe 5ae0b1175beb5d2b	f1bd2d46be619585 e47b9933bafdc655
t = 40: 5adbaa463642b570	e266c1f77d5ee90e	ec6d3abc2b291fd3	24c84b58d119affe
	83e8f410f859388e	d92f34c110296b32	9ecc381d277748a3	5ae0b1175beb5d2b
t =41: 50fdb7bb2e499a34 257ed8ea645e933a	5adbaa463642b570 83e8f410f859388e	e266c1f77d5ee90e d92f34c110296b32	ec6d3abc2b291fd3 9ecc381d277748a3
t = 42: 06514212bb7fa152	50fdb7bb2e499a34	5adbaa463642b570	e266c1f77d5ee90e
	466781db35181abe	257 ed8ea645e933a	83e8f410f859388e	d92f34c110296b32
t =43: 673ed5a55ff2b07d ba78f3545e7914f0	06514212bb7fa152 466781db35181abe	50fdb7bb2e499a34 257 ed8ea645e933a	5adbaa463642b570 83e8f410f859388e
t = 44: 125e2e5118393e2b	673 ed5a55ff2b07d	06514212bb7fa152	50fdb7bb2e499a34
	4453b23a3e13b090	ba78f3545e7914f0	466781db35181abe	257 ed8ea645e933a
t = 45: 07ee813df5910cec eae013a0510d23cc	125e2e5118393e2b 4453b23a3e13b090	673 ed5a55ff2b07d ba78f3545e7914f0	06514212bb7fa152 466781db35181abe
t = 46: 0a0508f0a1d719c3 a93815eb58891016	07ee813df5910cec eae013a0510d23cc	125e2e5118393e2b 4453b23a3e13b090	673 ed5a55ff2b07d ba78f3545e7914f0
t = 47: 0fc8f3b3efcb1b96	0a0508f0a1d719c3	07ee813df5910cec	125e2e5118393e2b
	a071cc73b966e801	a93815eb58891016	eae013a0510d23cc	4453b23a3e13b090
t = 48: 02aa5b28199f304a a49f1e14f8a2be7a	0fc8f3b3efcb1b96 a071cc73b966e801	0a0508f0a1d719c3 a93815eb58891016	07ee813df5910cec eae013a0510d23cc
t = 49: 9223e1b34382f104 bfe2106e512a7331	02aa5b28199f304a a49f1e14f8a2be7a	0fc8f3b3efcb1b96 a071cc73b966e801	0a0508f0a1d719c3 a93815eb58891016
t = 50: e01a1e47ee8d5656	9223e1b34382f104	02aa5b28199f304a	0fc8f3b3efcb1b96
	592b899b35469a78	bfe2106e512a7331	a49f1e14f8a2be7a	a071cc73b966e801
t = 51: fa7b17aad857c2f4	e01a1e47ee8d5656	9223e1b34382f104	02aa5b28199f304a
	eb6e85e4682c1671	592b899b35469a78	bfe2106e512a7331	a49f1e14f8a2be7a
t = 52: 0c523b7a3c84ab77 b5e80e871ac0c005	fa7b17aad857c2f4 eb6e85e4682c1671	e01a1e47ee8d5656 592b899b35469a78	9223e1b34382f104 bfe2106e512a7331
t = 53: c773d8b69da1fde2 be2b0602fc6f8f65	0c523b7a3c84ab77 b5e80e871ac0c005	fa7b17aad857c2f4 eb6e85e4682c1671	e01a1e47ee8d5656 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
	32ef50751734fee	1dab0bd116e434e5	c80bdc57f38a05e4	be2b0602fc6f8f65
t = 57: 1003ec42412c7b7d 1ec0d46f349fd058	8e3db3e380ec7f22 32ef50751734fee	bef9bb0fe467fd60 1dab0bd116e434e5	c6b1bc79a4f23679 c80bdc57f38a05e4
t = 58: 375facc76291f85e 59c8bc0488f9768b	1003ec42412c7b7d 1ec0d46f349fd058	8e3db3e380ec7f22 32ef50751734fee	bef9bb0fe467fd60 1dab0bd116e434e5
t = 59: bd113d92e0354fb9 e66c73db3fad397d	375facc76291f85e 59c8bc0488f9768b	1003ec42412c7b7d 1ec0d46f349fd058	8e3db3e380ec7f22 32ef50751734fee
t = 60: 2f61d4fd8e36d9d4	bd113d92e0354fb9	375facc76291f85e	1003ec42412c7b7d
	e9f21933e1c02948	e66c73db3fad397d	59c8bc0488f9768b	1ec0d46f349fd058
t = 61: 1b1ad88b92701ae2 6fd0c1719bcac335	2f61d4fd8e36d9d4 e9f21933e1c02948	bd113d92e0354fb9 e66c73db3fad397d	375facc76291f85e 59c8bc0488f9768b

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

Isso completa o processamento do segundo e último bloco de mensagem, M(2). O valor de hash final, H(2), é calculado para ser

$H_0^{(2)}$ = 2a7f1d895fd58e0b + deb3eeaa973bb9dd = 09330c33f71147e8

$H1^{(2)}$ = eaae96d1a673c741 + 526a98f5dc595406 = 3d192fc782cd1b47

$H2^{(2)}$ = 015a2173796c1a88 + 51b6f9a3c1ceeb4a = 53111b173b3b05d2

$H_3^{(2)}$ = f6352ca156acaff7 + 396b53e58d04471b = 2fa08086e3b0f712

$H4^{(2)}$ = c662113e9ebb4d64 + 3665b5dbb6c2e055 = fcc7c71a557e2db9

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

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

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

O valor de hash final é truncado para seus 384 bits mais à esquerda (ou seja, $H_0^{(1)}$,K, $H_5^{(1)}$), resultando em 384 bits resumo da mensagem

09330c33f71147e8 3d192fc782cd1b47 53111b173b3b05d2 2fa08086e3b0f712

fcc7c71a557e2db9 66c3e9fa91746039.

D.3 Exemplo SHA-384 (mensagem longa)

Seja a mensagem *M* a forma codificada em binário da string ASCII que consiste em 1.000.000 de repetições do caractere "a". O resumo da mensagem SHA-384 resultante é

9d0e1809716474cb 086e834e310a4a1c ed149e9c00f24852 7972cec5704c2a5b

07b8b3dc38ecc4eb ae97ddd87f3d8985.

APÊNDICE E: REFERÊNCIAS

[180-1] Federal Information Processing Standards (FIPS) Publicação 180-1, *Secure Hash Standard (SHS),* US DoC/NIST, 17 de abril de 1995.

[ESSE] A. Menezes, P. van Oorschot e S. Vanstone. *Handbook of Applied Cryptography,* CRC Press, Inc., outubro de 1997.