

SHA - Descrição e Resumo

**Pós Graduação Latu-Sensu
ITA/Stefanini**

**Rodrigo Rubira Branco
Criptografia
Prof. Faleiros**

1.0-) História

SHA quer dizer Secure Hash Algorithm e mostra-se como um dos mais utilizados algoritmos de Hash da atualidade.

SHA-0 foi inicialmente proposto na norma FIPS 180 (Maio, 1993) como o padrão para algoritmos de hash do governo norte-americano, sendo porém substituído pelo SHA1-1 na FIPS 180-1 (Abril, 1995) [1]. O SHA1 adiciona uma operação de rotação circular que aparentemente foi adicionada para superar as fraquezas apresentadas pelo SHA-0.

Atualmente, tanto o SHA-0 quanto o SHA-1 apresentam testes criptográficos aparentemente capazes de se gerar colisões (o SHA-1 devido as modificações incluídas, mostra-se mais resistente a tais situações, mas vem sendo colocado a prova constantemente). Devido a necessidades de resumos maiores, o NIST publicou outras funções de hash para a família do SHA [2], nomeadas SHA-256, SHA-384 e SHA-512 (com resumos de 256, 384 e 512 respectivamente). Tal publicação se deu em 2001, no esboço da norma FIPS 180-2 [3]. Em 2004 esta mesma norma foi modificada, para adicionar mais uma variante conhecida como SHA-224, criada para bater com o tamanho de duas chaves Triple DES (patente americana 6.829.355) [4].

2.0-) Descrição

Este artigo enfoca o SHA-1, por ser o mais amplamente difundido e utilizado na atualidade.

As operações matemáticas necessárias para o SHA, dado as palavras de 32 bits (x, y, z) e os operadores \wedge (AND), \vee (OR), $!$ (NOT), \oplus (XOR) e \ll (rotação circular para a esquerda – adicionado ao SHA1).

$$F(x,y,z) = (x \wedge y) \vee (!x \wedge z)$$

$$G(x,y,z) = x \oplus y \oplus z$$

$$H(x,y,z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$$

Salienta-se que o SHA utiliza-se de palavras de 32 bits, portanto as operações demonstradas deverão ser todas entendidas como módulo 32 e o mesmo também faz uso de notação “big-endian” [5].

3.0-) Passos do algoritmo

1. O SHA faz uso de blocos de bits de 512, precisando portanto complementar as entradas de forma a serem múltiplas deste valor.

Para X o número de bits de uma mensagem (M_s) da qual se deseja calcular o resumo e portanto $0 \leq X < \infty$.

Têm-se que a M_s será concatenado um bit com valor 1.

Concatena-se também a M_s a sequência de $[(447-X) \bmod 512]$ bits com o valor 0. Dado W uma palavra de 64 bits, faz-se $S = X \bmod (2 \text{ elevado a } 64)$.

Em M_s será concatenada a representação “big-endian” (conforme mencionado, o SHA entende que usa-se “big-endian” [5]) de S .

Desta forma, pode-se formar um M_s divisível por 512 conforme segue:

$\{M_s \text{ original}, 1, 0, 0, 0, \dots, 0, 0, 0, N \bmod (2 \text{ elevado } 64)\}$

Onde:

M_s original possui N bits

$N \bmod (2 \text{ elevado a } 64)$ possui 64 bits

E o restante possui $(447-N) \bmod 512$ bits

Após este procedimento, têm-se uma M_s divisível em blocos de 512 bits.

2. Definição das constantes Hexadecimais de 32 bits

A=6745.2301

B=EFCD.AB89

C=98BA.DCFE

D=1032.5476

E=C3D2.E1F0

3. Agora repete-se de 1 até o número de blocos de 512 bits que compõe o dado a ser feito hash

A2=A

B2=B

C2=C

D2=D

E2=E

4. Forma-se um bloco Msi composto de 16 palavras de 32 bits

5. Tendo-se W como um conjunto de 80 palavras de 32 bits, repete-se de 1 até 16 a atribuição:

$$W_{1...16} = M_{s1}...M_{s16}$$

6. Repete-se agora de 17 até 80:

$$W_{17...80} = (W_{\text{valor}-3} \oplus W_{\text{valor}-8} \oplus W_{\text{valor}-14} \oplus W_{\text{valor}-16})$$

7. Agora repete-se de 1 até 20:

$$T = (A \ll 5) + F(B, C, D) + E + W_{\text{valor}} + 5A82.7999$$
$$(E, D, C, B, A) = (D, C, B \ll 30, A, T)$$

8. Após, deve-se repetir de 21 até 40:

$$T = (A \ll 5) + G(B, C, D) + E + W_{\text{valor}} + 6ED9.EBA1$$
$$(E, D, C, B, A) = (D, C, B \ll 30, A, T)$$

9. De 41 até 60, faz-se:

$$T = (A \ll 5) + H(B, C, D) + E + W_{\text{valor}} + 8F1B.BCDC$$
$$(E, D, C, B, A) = (D, C, B \ll 30, A, T)$$

10. Finalmente, de 61 até 80 têm-se:

$$T = (A \ll 5) + G(B, C, D) + E + W_{\text{valor}} + CA62.C1D6$$
$$(E, D, C, B, A) = (D, C, B \ll 30, A, T)$$

$$11. (A, B, C, D, E) = (A + A2, B + B2, C + C2, D + D2, E + E2)$$

12. Para terminar, obtém-se o hash final através da concatenação dos valores de A, B, C, D e E.

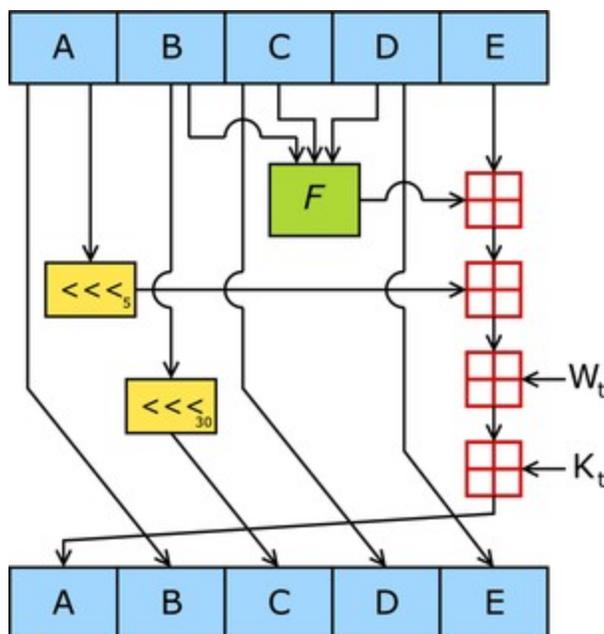


Figura 1. Uma das interações da função de compressão SHA-1.

Índice de Figuras:

- Figura1: Interação do SHA-1

Fonte: <http://en.wikipedia.org/wiki/Image:SHA-1.png>

Referências:

[1] Página sobre hashes criptográficos do NIST,

<http://csrc.nist.gov/CryptoToolkit/tkhash.html>. Acessado em: 06/06/2006.

[2] Página descrevendo as diferenças entre os diversos hashes da família SHA,

<http://en.wikipedia.org/wiki/SHA-2>. Acessado em: 06/06/2006.

[3] Revisão da norma FIPS 180-2, <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>. Acessado em: 06/06/2006.

[4] RFC sobre o SHA-224, <ftp://ftp.rfc-editor.org/in-notes/rfc3874.txt>. Acessado em: 06/06/2006.

[5] Página explicativa sobre little/big endian,

<http://www.cs.umass.edu/~verts/cs32/endian.html>. Acesso em: 06/06/2006.