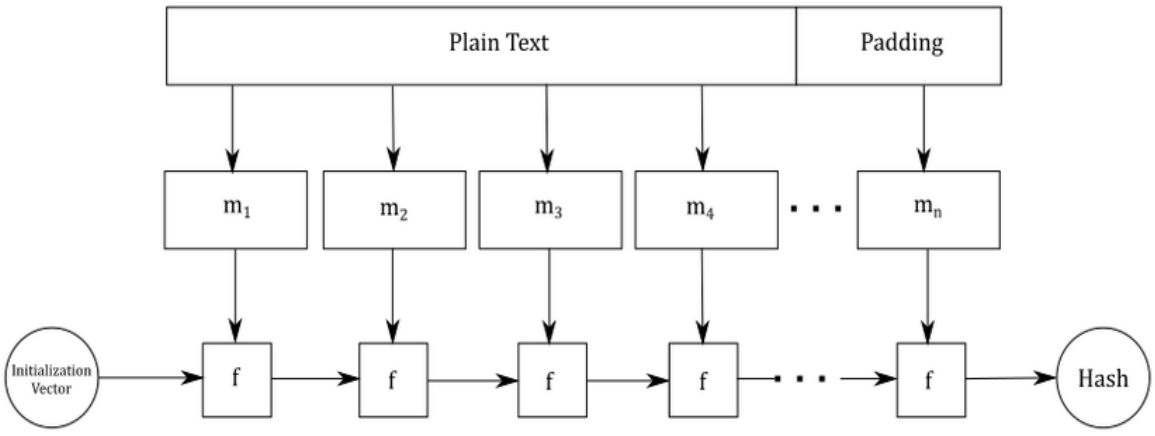
ANALYSIS OF SHA-1 HASH FUNCTION ALGORITHM

Mirzaxmedova E'zozaxon
National University of Uzbekistan named after Mirzo Ulugbek
Master student in the Department of information security

Abstract In the field of information security, hashing algorithms play an important role in ensuring the integrity and confidentiality of data. One of the most widely used hashing algorithms available today is the Secure Hash Algorithm (SHA-1). The hashing process in the SHA-1 algorithm consists of two main steps: initial processing of the plaintext (completing the message and dividing it into blocks), calculating the hash value. This article describes each step of the hash algorithm separately and shows how to reverse the steps to determine the plaintext from the hash value.

Keywords: SHA-1, plaintext, hash value, initial hash value, K_t constants, logical functions.

SHA - Secure Hash Algorithm was published by National University of Standards and Technologies (NIST) in the USA in 1992 in the form of the Federal Information Processing Standard - **PUB FIPS 180**, and was revised in 1995. It was called **SHA-1.** The SHA algorithm is based on the MD4 algorithm and is very similar in structure. The SHA-1 algorithm is based on the **MDC – Merkle Damgard Construction** (pic. 1).



Picture 1. MDC diagram

$l(M)$ – less than 2^{64}.

$H^{(i)}$ – 160 bits.

Number of rounds – 80.

1. Parameters and operations of SHA-1 algorithm

1.1. Parameters

$\boldsymbol{A, B, C, D, E}$ – variables with 32-bit length used to calculate $H^{(i)}$ hash value;

$\boldsymbol{H^{(i)}}$ – i-hash value. $H^{(0)}$ – initial hash value; $H^{(N)}$ – final hash value;

$\boldsymbol{H_j^{(i)}}$ – j-word of i-hash value;

$\boldsymbol{K_t}$ – constant value used for t iterations of the hash value calculation;

$\boldsymbol{k}$ – the number of zeros to be added at the message expansion stage;

$\boldsymbol{l}$ – length of M data in bits;

$\boldsymbol{m}$ – the number of bits of $M^{(i)}$ message block;

$\boldsymbol{M}$ – message to be hashed;

$\boldsymbol{M^{(i)}}$ – message block i with length m;

$\boldsymbol{M_j^{(i)}}$ – j-word of i-message block;

$\boldsymbol{N}$ – the number of blocks in the extended message;

$\boldsymbol{W_t}$ – t-word of the message table.

1.2. Operations

∧ – bitwise AND operation;

∨ – bitwise OR operation;

⊕ – bitwise XOR operation;

¬ – bitwise NOT operation

⋘ – shift left.

Table 1. Truth table.

x	y	$\neg x$	$x \wedge y$	$x \vee y$	$x \oplus y$

1	1	0	1	1	0
1	0	0	0	1	1
0	1	1	0	1	1
0	0	1	0	0	0

2. Steps to calculate the hash value:

2.1. Expand the message:

Let the length of M information be equal to l. The message length is expanded by a factor of 512. After the length of the data, one bit equal to 1 is added and k zeros are written. k is determined as follows: $k \equiv (448 - (l + 1))mod\ 512$. The remaining 64 bits are written with the value of the information length – l in binary form. Padding is always performed even if the data length is comparable to 448 by 512 modules.[21]

2.2. Dividing the extended message into blocks:

The extended message is divided into 512-bit blocks $M^{(1)}, M^{(2)}, \dots, M^{(N)}$.

2.3. Preparation of message table[22]:

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

2.4. Initial hash value:

The appearance of the initial hash values for the SHA-1 algorithm in the 16-digit system is as follows[23]:

$$H_0^{(0)} = 67452301$$

$$H_1^{(0)} = EFCDAB89$$

$$H_2^{(0)} = 98BADCFE$$

$$H_3^{(0)} = 10325476$$

$$H_4^{(0)} = C302E1F0$$

[21] D.Y. Akbarov. Axborot xavfsizligni ta'minlashning kriptografik usullari va ularning qo'llanilishi. – VII bob. Hesh funksiya va uning axborotni muhofazalash masalalarini yechishdagi qo'llanishlari.
[22] Federal Information Processing Standards (FIPS) Publication 180, 180-1, 180-2, 180-3, 180-4. Secure Hash Standard
[23] Federal Information Processing Standards (FIPS) Publication 180, 180-1, 180-2, 180-3, 180-4. Secure Hash Standard

2.5. Logical functions[24]*:*

$$f_t(x,y,z) = \begin{cases} (x \wedge y) \vee (\neg x \wedge z) & 0 \le t \le 19 \\ x \oplus y \oplus z & 20 \le t \le 39,\ 60 \le t \le 79 \\ (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) & 40 \le t \le 59 \end{cases}$$

2.6. Constants:

The appearance of K_t constants for the SHA-1 algorithm in the 16-digit number system is as follows[25]:

$$K_t = \begin{cases} 5A827999, & 0 \le t \le 19 \\ 6ED9EBA1, & 20 \le t \le 39 \\ 8F1BBCDC, & 40 \le t \le 59 \\ CA62C1D6, & 60 \le t \le 79 \end{cases}$$

2.7. Create buffers A, B, C, D, E using $i-1$ *hash value:*

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

$B = H_1^{(i-1)}$

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

$D = H_3^{(i-1)}$

$E = H_4^{(i-1)}$

2.8. Main cycle[26]*:*

for $t = 0$ to 79:

{

$T = (A \lll 5) + f_t(B,C,D) + E + K_t + W_t$

$E = D$

$D = C$

$C = B \lll 30$

$B = A$

$A = T$

[24] Federal Information Processing Standards (FIPS) Publication 180, 180-1, 180-2, 180-3, 180-4. Secure Hash Standard

[25] Federal Information Processing Standards (FIPS) Publication 180, 180-1, 180-2, 180-3, 180-4. Secure Hash Standard

[26] Federal Information Processing Standards (FIPS) Publication 180, 180-1, 180-2, 180-3, 180-4. Secure Hash Standard, D.Y. Akbarov. Axborot xavfsizligni ta'minlashning kriptografik usullari va ularning qo'llanilishi. – VII bob. Hesh funksiya va uning axborotni muhofazalash masalalarini yechishdagi qo'llanishlari

}

2.9. Calculate the i-hash value $H^{(i)}$:

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

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

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

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

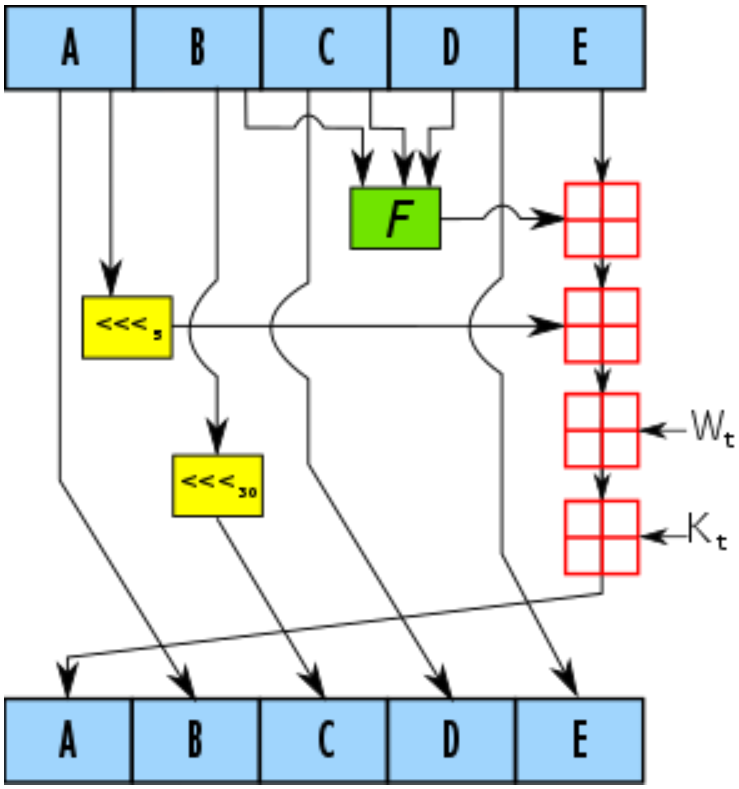
$$H_4^{(i)} = E + H_4^{(i-1)}$$

2.10.The hash value is determined as follows:

After repeating the above steps N times (for $M^{(N)}$), the final 160-bit result is obtained as a hash value[27]:

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

3. A single round scheme in the SHA-1 algorithm:



[27] Federal Information Processing Standards (FIPS) Publication 180, 180-1, 180-2, 180-3, 180-4. Secure Hash Standard, D.Y. Akbarov. Axborot xavfsizligni ta'minlashning kriptografik usullari va ularning qo'llanilishi. – VII bob. Hesh funksiya va uning axborotni muhofazalash masalalarini yechishdagi qo'llanishlari

Picture 2. A single round scheme in the SHA-1 algorithm

4. Return to the plaintext

4.1. Lets $H = H_0{}^N H_1{}^N H_2{}^N H_3{}^N H_4{}^N$ *– hash value of M message*

$A = H_0{}^i - H_0{}^{i-1}$

$B = H_1{}^i - H_1{}^{i-1}$

$C = H_2{}^i - H_2{}^{i-1}$

$D = H_3{}^i - H_3{}^{i-1}$

$E = H_4{}^i - H_4{}^{i-1}$

4.2. Main cycle:

for $t = 79$ to 0:

{

$T = A$

$A = B$

$B = C \ggg 30$

$C = D$

$D = E$

$E = T - (A \ggg 5) - f_t(B, C, D) - K_t - W_t$

$W_t = T - (A \ggg 5) - f_t(B, C, D) - K_t - E$

}

All W_t are determined by following the steps above.

REFERENCES:

1. Federal Information Processing Standards (FIPS) Publication 180-2. Secure Hash Standard (SHS). 2002 August 1.

2. Federal Information Processing Standards (FIPS) Publication 180-3. Secure Hash Standard (SHS). October 2008.

3. Federal Information Processing Standards (FIPS) Publication 180-4. Secure Hash Standard (SHS). March 2012.

4. Federal Information Processing Standards (FIPS) Publication 180-1. Secure Hash Standard (SHS). 1995 April 17.

5. Federal Information Processing Standards (FIPS) Publication 180. Secure Hash Standard (SHS). 1993 May 11.

6. Federal Information Processing Standards (FIPS) Publication 180-4. Secure Hash Standard (SHS). August 2015.

7. Christof Paar and Jan Pelzl. Understanding Cryptography – A textbook for students and practitioners. Chapter 11 – Hash Functions. 2009 October 29.

8. D. Y. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi. – Toshkent, “O‘zbekiston markasi” nashriyoti, 2009 – 432 bet.