

SECURE HASH ALGORITHM (SHA)

The Secure Hash Algorithm (SHA) was proposed as part of the digital signature standard. SHA-1, the first version of this standard, takes messages with a maximum length of 2^{24} and produces a 160-bit digest. With this algorithm, SHA-1 uses five registers, R_1 through R_5 , to maintain a "state" of 20 bytes.

The first step is to pad a message m with length l_m . The message length is forced to $l_m = 448 \bmod 512$. In other words, the length of the padded message becomes 64 bits less than the multiple of 512 bits. The number of padding bits can be as low as 1 bit and as high as 512 bits. The padding includes a 1 bit and as many 0 bits as required. Therefore, the least-significant 64 bits of the message length are appended to convert the padded message to a word with a multiple of 512 bits.

After padding, the second step is to expand each block of 512-bit (16 32 bits) words $\{m_0, m_1, \dots, m_{15}\}$ to words of 80 32 bits using:

Equation 5.12

$$w_i = m_i \text{ for } 0 \leq i \leq 15$$

and

Equation 05.13

$$w_i = w_{i-3} \oplus w_{i-8} \oplus w_{i-14} \oplus w_{i-16} \leftarrow 1 \text{ for } 16 \leq i \leq 79,$$

where $\leftarrow j$ means left rotation by j bits. This way, bits are shifted several times if the incoming block is mixed with the state. Next, bits from each

block of w_i are mixed into the state in four steps, each maintaining 20 rounds. For any values of a , b , and c , and bit number i , we define a function $F_i(a, b, c)$ as follows:

Equation 05.14

$$F_i(a, b, c) = \begin{cases} (a \cap b) \cup (\bar{a} \cap c) & 0 \leq i \leq 19 \\ a \oplus b \oplus c & 20 \leq i \leq 39 \\ (a \cap b) \cup (a \cap c) \cup (b \cap c) & 40 \leq i \leq 59 \\ a \oplus b \oplus c & 60 \leq i \leq 79 \end{cases}$$

Then, the 80 steps ($i = 0, 1, 2, \dots, 79$) of the four rounds are described as follows:

Equation 05.15

$$\delta = (R_1 \leftrightarrow 5) + F_i(R_2, R_3, R_4) + R_5 + w_i + C_i$$

Equation 05.16

$$R_5 = R_4$$

Equation 05.17

$$R_4 = R_3$$

Equation 05.18

$$R_3 = R_2 \leftrightarrow 30$$

Equation 05.19

$$R_2 = R_1$$

Equation 05.20

$$R_1 = \delta,$$

where C_i is a constant value specified by the standard for round i . The message digest is produced by concatenation of the values in R_1 through R_5 .

Authentication and Digital Signature

A digital signature is one of the most important required security measures. Much like a person's signature on a document, a digital signature on a message is required for the authentication and identification of the right sender. The digital signature is supposed to be unique to an individual and serves as a means of identifying the sender. An electronic signature is not as easy as it was with the paper-based system. The digital signature requires a great deal of study, research, and skill. Even if these requirements are met, there is no guarantee that all the security requirements have been met.

The technical method of providing a sender's authentication is performed through cryptography. Many cryptographic mechanisms have been developed. Among them, the RSA algorithm implements both encryption and digital signature. When RSA is applied, the message is encrypted with the sender's

private key. Thus, the entire encrypted message serves as a digital signature. This means that at the receiving end, the receiver can decrypt it, using the public key. This authenticates that the packet comes from the right user.

Source : <http://elearningatria.files.wordpress.com/2013/10/cse-vi-computer-networks-ii-10cs64-notes.pdf>