FIPS 180-2, SECURE HASH STANDARD
CHANGE NOTICE 1

U.S. DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Gaithersburg, MD 20899

DATE OF CHANGE: year month day

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

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

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size (bits)	Security (bits)
SHA-224	$< 2^{64}$	512	32	224	112

Questions regarding this change notice may be directed to Elaine Barker (Email: ebarker@nist.gov, Phone: 301-975-2911).

1 SHA-224 Specification

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

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

$$H_0^{(0)} = \texttt{c1059ed8}$$

$$H_1^{(0)} = \texttt{367cd507}$$

$$H_2^{(0)} = \texttt{3070dd17}$$

$$H_3^{(0)} = \texttt{f70e5939}$$

$$H_4^{(0)} = \texttt{ffc00b31}$$

$$H_5^{(0)} = \texttt{68581511}$$

$$H_6^{(0)} = \texttt{64f98fa7}$$

$$H_7^{(0)} = \texttt{befa4fa4}$$

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

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

2 SHA-224 Examples

2.1 SHA-224 Example (One-Block Message)

[To be provided]

2.2 SHA-224 Example (Multi-Block Message)

[To be provided]

2.3 SHA-224 Example (Long Message)

[To be provided]