SHA1 Encryption Algorithm

ADI - AMD
ARM - DSP Group
LSI Logic ZSP
MIPS - TI

VOCAL Technologies, Ltd. software libraries include a complete range of ETSI / ITU / IEEE compliant algorithms, optimized for execution on ANSI C and leading DSP architectures (ADI, AMD-Alchemy, ARM, DSP Group, LSI Logic ZSP, MIPS and TI).

The SHA1 encryption algorithm specifies a Secure Hash Algorithm (SHA1), which can be used to generate a condensed representation of a message called a message digest. The SHA1 is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required. Both the transmitter and intended receiver of a message in computing and verifying a digital signature uses the SHA1.

SHA1 is used for computing a condensed representation of a message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature

The SHA1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA1 is a technical revision of SHA (FIPS 180). A circular left shift operation has been added to the SHA (FIPS 180). SHA1 improves the security provided by the SHA standard. The SHA1 is based on principles similar to those used by the MD4 message digest algorithm.

SHA1 Features:

- The SHA1 is used to compute a message digest for a message or data file that is provided as input.
- The message or data file should be considered to be a bit string.
- The length of the message is the number of bits in the message (the empty message has length 0).
- If the number of bits in a message is a multiple of 8, for compactness we can represent the message in hex.
- The purpose of message padding is to make the total length of a padded message a multiple of 512.
- The SHA1 sequentially processes blocks of 512 bits when computing the message digest.
- As a summary, a "1" followed by m "0"s followed by a 64-bit integer are appended to the end of the message to produce a padded message of length 512 * n.
- The 64-bit integer is l, the length of the original message.
- The padded message is then processed by the SHA1 as n 512-bit blocks.

SHA1 Implementations:

- VOCAL Technologies, Ltd. SHA1 is implemented in software, hardware and with UDI instructions.
- VOCAL Technologies, Ltd. also offers SHA2 (FIPS 180-2 August 2002)
- For more information about the different implementations contact David Jamieson at (716) 688-4675 or http://www.vocal.com

Custom Product Design Division
200 John James Audubon Parkway
Buffalo, New York 14228
716-688-4675
http://www.vocal.com/