http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html Go MAY JUN JUL
267 captures 25
11 Oct 2007 - 27 Oct 2020 2010 2011 2012
About this capture

National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC: GO

CSRC HOME GROUPS PUBLICATIONS DRIVERS NEWS & EVENTS ARCHIVE

CRYPTOGRAPHIC TOOLKIT
- Block Ciphers
- Block Cipher Modes
- Digital Signatures
- Entity Authentication
- Implementation Guideline
- Key Derivation Functions
- Key Management
- Message Authentication
- Password Usage and Generation
- Random Number Generation
- Secure Hashing
  - Approved Algorithms
  - Testing / Products
  - Additional Information
- Algorithm Examples

CSRC HOME > GROUPS > ST > CRYPTOGRAPHIC TOOLKIT

SECURE HASHING

Approved Algorithms

There are five (5) ***Approved*** algorithms for generating a condensed representation of a message (message digest): ***SHA-1, SHA-224, SHA-256, SHA-384***, and ***SHA-512***.

February 11, 2011: NIST announces the release of draft Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard (SHS). Draft FIPS 180-4 is a proposed revision of FIPS 180-3. Draft FIPS 180-4 adds a general procedure for creating an initialization hash value and two additional secure hash algorithms: SHA-512/224 and SHA-512/256, and removes a requirement that padding must be done before hash computation begins. SHA-512/224 and SHA-512/256 may be more efficient alternatives to SHA-224 and SHA-256, respectively, on platforms that are optimized for 64-bit operations. Removing the restriction on the padding operation in the secure hash algorithms will potentially create more flexibility and efficiency in implementing the secure hash algorithms in many computer network applications. The Federal Register Notice (FRN) of this publication is located here. Examples of the implementation of the secure hash algorithms SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256, can be found at http://www.nist.gov/CryptoToolkitExamples.

March 15, 2006: The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms. Federal agencies should stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010. After 2010, Federal agencies may use SHA-1 only for the following applications: hash-based message authentication codes (HMACs); key derivation functions (KDFs); and random number generators (RNGs). Regardless of use, NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.

SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512

FIPS 180-3, Secure Hash Standard (SHS), October 2008

FIPS 180-3 is a revision of FIPS 180-2. The FIPS specifies five secure hash algorithms for use in computing a condensed representation, called a message digest, of electronic data. The technical information about the security provided by the secure hash algorithms, and the length limits and security implications of truncated hash outputs is provided in Special Publication 800-107, Recommendation for Applications Using Approved Hash Algorithms.

In August, 2004, researchers announced that they discovered a new way to break a number of cryptographic hash algorithms. Those initial attacks did not break any of the SHA family algorithms, as is reflected in NIST's comments at that time.

In February, 2005, however, researchers announced an attack on the full SHA-1 algorithm. Click here for NIST's brief comments on these latest attacks. (Statement revised April 25, 2006.)

NIST announces the release of Special Publication 800-106, Randomized Hashing for Digital Signatures. This Recommendation provides a technique to randomize the input messages to hash functions prior to the generation of digital signatures to strengthen security of the digital signatures.

NIST announces the release of the Special Publication 800-107, Recommendation for Using Approved Hash Algorithms. This Recommendation provides guidance on using the Approved hash algorithms in digital signatures applications, Keyed-hash Message Authentication Codes (HMACs), key derivation functions (KDFs) and random number generators.

Back to Top

Testing Products

Testing requirements and validation lists are available from the Cryptographic Algorithm Validation Program (CAVP).

Back to Top

Additional Information

NIST is currently conducting a competition to develop a new cryptographic hash algorithm. For more infomation on this competition and other hash related issues please see the Cryptographic Hash Project page.

April 12, 2011: NIST requested comments for Draft Special Publication (SP) 800-131B, Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths. on February 10, 2001. SP 800-131B provides details about the validation of the cryptographic algorithms and cryptographic modules in transition, as specified in SP 800-131A. These are the comments received.

April 12, 2011: NIST requested comments for Draft Special Publication (SP) 800-131C, Transitions: Validating the Transition from FIPS 186-2 to FIPS 186-3 on February 10, 2011. SP 800-131C addresses both the cryptographic algorithm validations and the cryptographic module validations that are conducted by

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html Go MAY JUN JUL
267 captures
11 Oct 2007 - 27 Oct 2020
2010 25 2011 2012
About this capture

Cryptographic Module Validation Program (CMVP), respectively. These are the comments received.

January 13, 2011: NIST announces the completion of Special Publication (SP) 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. This Recommendation provides the approach for transitioning from the use of one algorithm or key length to another, as initially addressed in Part 1 of SP 800-57. SP 800-131B, Transitions: Validation of Transitioning Cryptographic Algorithms and Key Lengths, is under development and will address the validation of cryptographic modules during the transition period.

Note: An algorithm or technique that is either specified in a FIPS or NIST Recommendation.

CryptoToolkit Webmaster, Disclaimer Notice & Privacy Policy
NIST is an Agency of the U.S. Department of Commerce

Last updated: April 12, 2011
Page created: December 21, 2000

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.