ITL BULLETIN FOR MAY 2012

SECURE HASH STANDARD: UPDATED SPECIFICATIONS APPROVED AND ISSUED AS FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 180-4

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Department of Commerce

Cryptographic methods provide strong ways to protect information technology (IT) systems, applications, and information. Organizations using cryptographic methods can maintain the confidentiality and integrity of information, verify that information was not changed after it was sent, and authenticate the originator of the information. Modern cryptography uses mathematical techniques and relies upon two basic components: an algorithm (or cryptographic methodology) and a cryptographic key, which determines the specifics of algorithm operation.

Hash algorithms are used as components by other cryptographic algorithms and processes to provide information security services. Hash functions are often utilized with digital signature algorithms, keyed-hash message authentication codes, key derivation functions, and random number generators. A hash algorithm converts a variable length message into a condensed representation of the electronic data in the message. This representation, or message digest, can then be used for digital signatures, message authentication, and other secure applications. When employed in a digital signature application, the hash value of the message is signed instead of the message itself; the receiver can use the signature to verify the signer of the message and to authenticate the integrity of the signed message.

Recently, the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) completed a revision of the federal government's standard for secure hash functions. Issued as Federal Information Processing Standard (FIPS) 180-4, *Secure Hash Standard (SHS)*, and approved by the Secretary of Commerce in March 2012, the revised standard replaces FIPS 180-3 and specifies seven secure hash algorithms.

To maintain the strength of cryptographic algorithms as new threats to systems and information emerge, NIST has been conducting an open, public competition to develop a new, robust cryptographic hash algorithm. When the new algorithm has been selected and approved, it will augment the hash algorithms that are currently included in FIPS 180-4.

Changes Implemented in FIPS 180-4, *Secure Hash Standard (SHS)*

FIPS 180-4 provides seven secure hash algorithms (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256) for computing a condensed representation of electronic data. SHA–512/224 and SHA–512/256 were added to the standard, augmenting the five algorithms that had been identified in FIPS 180–3, which was issued in 2008. SHA-512/224 and SHA-512/256 are based on SHA-512, but use different initialization vectors and truncate the final SHA-512 output to 224 and 256 bits, respectively. They may be more efficient alternatives to SHA–224 and SHA–256, respectively, on platforms that are optimized for 64-bit operations.

When a message of any length less than 2^{64} bits (for SHA-1, SHA-224, and SHA-256) or less than 2^{128} bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash

algorithm, the resulting message digests range in length from 160 to 512 bits, depending on the algorithm used.

The algorithms differ significantly in the security strengths that they provide to the data being hashed. NIST Special Publication (SP) 800-57, *Recommendation for Key Management*, and SP 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, explain the security strengths of the hash functions and the security of the information system when each of the hash algorithms is used with other cryptographic algorithms, including digital signature algorithms and keyed-hash message authentication codes. See the publication listing in the **For More Information** section below.

The hash algorithms specified in the revised standard provide security because, for a given algorithm, it is not computationally feasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest. Any change to a message will most likely result in a different message digest. This will cause a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm.

The revised standard also updates the procedures for producing a condensed representation of an electronic message by removing a restriction that padding must be done before the hash computation begins. Padding ensures that the resulting message is a multiple of 512 or 1024 bits, depending on the algorithm used. Padding can be inserted before the hash computation begins on a message, or at any other time during the hash computation prior to processing the block(s) that will contain the padding. By removing the restriction on the padding operation in the secure hash algorithms, the revised standard provides for more flexibility and efficiency in the implementation of the secure hash algorithms in many computer network applications.

Review and Approval of FIPS 180-4

NIST announced the draft of FIPS 180-4 in a February 2011 *Federal Register* notice that solicited comments on the proposed revision from the public, research communities, manufacturers, voluntary standards organizations, and federal, state and local government organizations. NIST reviewed the comments and added clarifications to the proposed revised standard. The *Federal Register* notice announcing the approval of FIPS 180-4, including an analysis of the comments received, is available here.

FIPS 180-4, which was effective March 6, 2012, is available here.

Validation of Hash Algorithms

The secure hash algorithms specified in FIPS 180-4 may be implemented in software, firmware, hardware, or any combination thereof. Implementations of secure hash algorithms used by federal government agencies must be tested for conformance to the standard and validated by the NIST Cryptographic Algorithm Validation Program (CAVP).

The CAVP covers validation testing for FIPS-approved and NIST-recommended cryptographic algorithms, and is a component of the Cryptographic Module Validation Program (CMVP). This program was established by NIST and the Communications Security Establishment Canada (CSEC) in July 1995 to validate the cryptographic modules that contain cryptographic algorithms. These algorithms are used in products and systems to provide security services, such as

confidentiality, integrity, and authentication. The testing and validation of cryptographic modules and their underlying cryptographic algorithms provide organizations with assurance that their data and systems are safely protected.

FIPS 140-2, *Security Requirements for Cryptographic Modules*, provides for the secure design and implementation of cryptographic modules. The cryptographic module is the hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms, and is contained within a defined cryptographic boundary.

All of the tests conducted under the CAVP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in having their algorithm implementations validated may select from the list of accredited laboratories for the testing process. Information about the validation program, including testing requirements and validation lists for secure hash algorithm implementations, is available here.

Cryptographic Toolkit

FIPS and NIST Recommendations, which are issued as Special Publications (SPs), specify cryptographic algorithms; cryptographic hash functions; techniques for protecting the keys used in the cryptographic processes; methods that are used for authentication and integrity detection; and techniques for generating random numbers that are used in many cryptographic applications.

These techniques are part of a comprehensive Cryptographic Toolkit that NIST has developed to help federal government agencies and other organizations select effective cryptographic security components and processes that will protect their IT data, communications, and operations. The toolkit currently includes a wide variety of cryptographic algorithms and techniques, and more will be added in the future. Information about the toolkit can be found here.

Transition from FIPS 180-3 to FIPS 180-4

Guidance concerning the testing and validation of hash algorithms for conformance to FIPS 180-4 and the relationship with FIPS 140-2 can be found in the Cryptographic Module Validation Program (CMVP) management and implementation guides here.

Selection of the New SHA-3

In November 2007, NIST started an open, public process to solicit candidates for a new and robust cryptographic hash algorithm for use by federal government agencies in protecting their information systems and information. An invitation was issued to organizations and individuals to submit candidate algorithms for a new hash algorithm, referred to as SHA-3.

The first round of the Cryptographic Hash Algorithm Competition began in November 2008 after NIST had received 64 entries for the competition as a result of the 2007 announcement inviting candidates. The entries were reviewed, and 51 of the submissions were announced in December 2008 as meeting the minimum submission requirements. At a conference held in 2009, submitters of the 51 candidate algorithms were invited to present their algorithms. NIST discussed the competitive process and the criteria for selecting the second-round candidates, which would be subject to further study. In July 2009, NIST announced 14 second-round candidates that were

made available for public review. At a second-round conference held in 2010, the security and performance analyses of the 14 candidates were discussed.

NIST received many views from the cryptographic community, both before and after the conference. Based on this public feedback and the internal reviews of the second-round candidates, NIST selected five finalists to advance to the third, and final, round of the competition.

The five SHA finalist algorithms were available for public review for one year after they were announced in December 2010, and were discussed at a final candidate conference held in March 2012. NIST expects to select the final SHA-3 later in 2012. Information about the SHA-3 competition is available here.

For More Information

The following Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) are referenced in FIPS 180-4:

FIPS 140-2, *Security Requirements for Cryptographic Modules*

FIPS 180-3, *Secure Hash Standard (SHS)*

NIST SP 800-57, *Recommendation for Key Management.* This publication provides background information and establishes frameworks to support the selection and use of cryptographic mechanisms. The security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. SP 800-57 advises developers and system administrators on secure practices for generation, storage, distribution, and destruction of keys, and helps system owners and managers in establishing effective key management practices within their organizations.

NIST SP 800-107, *Recommendation for Applications Using Approved Hash Algorithms.* This publication explains the properties of hash functions and how the security strength of the hash algorithm is determined. SP 800-107 also discusses a standard method for truncating cryptographic hash function outputs or message digests. This information helps implementers and application developers build applications that may require a message digest that is shorter than the full-length message digest. The publication includes guidelines on choosing the length of the truncated message digest based on application-related considerations and the security implications of the selections. Other topics addressed in SP 800-107 include the use of the hash function in digital signatures, message authentication, key derivation functions, and random number generation.

For information about these NIST standards and recommendations, as well as other security-related publications, see NIST's web page here.

ITL Bulletin Publisher: Elizabeth Lennon
Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email here.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.