THE CRYPTOGRAPHIC HASH ALGORITHM FAMILY: REVISION OF THE SECURE HASH STANDARD AND ONGOING COMPETITION FOR NEW HASH ALGORITHMS

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

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 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) 180-3, *Secure Hash Standard*, and approved by the Secretary of Commerce in October 2008, the revised standard replaces FIPS 180-2 and specifies five secure hash algorithms.

Because recent advances in the cryptanalysis of hash functions could threaten the security of cryptographic processes, NIST is conducting an open, public competition to develop a new, robust cryptographic hash algorithm. When the new algorithm is developed, evaluated, and approved, it will augment the hash algorithms currently specified in FIPS 180-3.

Federal Information Processing Standard (FIPS) 180-3, *Secure Hash Standard*

FIPS 180-3 includes the four hash algorithms that had been specified in the former *Secure Hash Standard* (FIPS 180-2) and incorporates an additional algorithm that had been specified in Change Notice 1 to FIPS 180-2. In addition, the description of a truncation method that had been provided in the Change Notice was incorporated into the revised standard. The five algorithms approved for computing a message digest are SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

These five algorithms differ in the size of the blocks and words of data that are used to carry out the hashing process. Messages of less than 2^{64} bits in length (for SHA-1, SHA-224, and SHA-256) or less than 2^{128} bits in length (for SHA-384 and SHA-512) are processed by the hash algorithms to produce message digests of 160, 224, 256, 384, and 512 bits, respectively. The algorithms also vary in the security strengths that they provide.

Information about the specifications for FIPS 180-3, including requirements for the validation of cryptographic modules implementing hash algorithms, is available from the NIST Web page http://csrc.nist.gov/publications/PubsFIPS.html.

The secure hash algorithms are components of NIST's Cryptographic Toolkit that helps federal and private sector organizations select cryptographic security components and processes to protect their data, communications, and operations. Information about the toolkit, which includes a variety of cryptographic algorithms and techniques, can be found at http://csrc.nist.gov/groups/ST/toolkit/index.html.

Security Strengths of Hash Functions

A secure hash function is a collision-resistant, one-way function. Collision resistance means that it is extremely difficult to find two different messages that will produce the same hash value. One way means that it is easy to compute the hash value from the input, but it is extremely difficult to reproduce the input from the hash value, or to find another input that will produce the same hash value.

Hash functions are often used to determine whether or not data has changed. Many algorithms and processes that provide a security service use a hash function as a component of the algorithm or process, including:

- Keyed-hash message authentication code (HMAC)
- Digital signatures
- Key derivation functions (KDFs)
- Random number generators (RNGs)

Because cryptanalysts have found ways to attack commonly used hash functions, NIST has advised federal agencies to stop as soon as practical the use of the SHA-1 algorithm for digital signatures, digital timestamping, and other applications that require collision resistance, and to use the SHA-2 family of hash functions for these applications after 2010. SHA-1 may be used only for hash-based message authentication codes, key derivation functions, and random number generators after 2010. NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.

To keep users and developers up to date on the potential threats to the security of hash algorithms, NIST has issued recommendations about the security strengths of the five approved hash algorithms in a publication that can be modified and updated in a timely manner to provide current information.

Recommendations for Use of Hash Algorithms

NIST Special Publication (SP) 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, written by Quynh Dang of NIST, explains the properties of

hash functions and how the security strength of the hash algorithm is determined. The publication 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 presents 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.

Another new publication, NIST SP 800-106, *Randomized Hashing for Digital Signatures*, also written by Quynh Dang, recommends a technique to randomize messages that are input to a cryptographic hash function during the generation of digital signatures using the Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and Rivest-Shamir-Adleman (RSA). Collision resistance is a required property for the cryptographic hash functions used in digital signature applications. The randomization method presented in SP 800-106 strengthens the collision resistance provided by the cryptographic hash functions in digital signature applications without any changes to the core cryptographic hash functions and digital signature algorithms. A message will have a different digital signature each time it is signed if it is randomized with a different random value.

General guidance to organizations in their selection and use of cryptographic mechanisms to provide security for protocols and applications is addressed in NIST SP 800-57, *Recommendation for Key Management*.

NIST Special Publications are available from the Web page http://csrc.nist.gov/publications/PubsSPs.html.

Competition to Develop a New Cryptographic Hash Algorithm

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 to submit candidate algorithms was issued, with nominations to be submitted to NIST by October 31, 2008. The new hash algorithm, to be called SHA-3, will augment the hash algorithms currently specified in FIPS 180-3, *Secure Hash Standard*.

Information about the NIST Cryptographic Hash Competition is available at http://www.nist.gov/hash-competition.

A *Federal Register* notice (Vol. 72, No. 212, pp. 62212-20) published on November 2, 2007, provided the nomination requirements and the minimum acceptability requirements for the new algorithm. The notice also included the evaluation criteria that will be used to assess the nominations. The November Federal Register notice is available on NIST's Web page http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf.

NIST received 64 entries for the hash algorithm competition. After an internal review of the submissions, 51 were selected for meeting the minimum submission requirements and were accepted as the first round candidates. NIST invites public review of the candidate algorithms. Information about the candidate algorithms and about the submission of comments is available at http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html.

NIST will periodically post and update the comments that are received about the algorithms.

First SHA-3 Candidate Conference

Submitters of the 51 first round candidate algorithms were invited to participate in the First SHA-3 Candidate Conference at KU Leuven, Belgium in February 2009, and to present their algorithms to the participants. Presentation materials used by the submitters who participated, as well as information prepared by those who were not able to participate, can be viewed on the Web page http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/program.html.

In addition to candidates' presentations, NIST held four discussion sessions on several technical issues to obtain public feedback. NIST also briefed conference attendees on its plan to select about 15 second round candidates by summer 2009, and discussed the criteria for this process. Public comments on the first round candidates should be received by June 1, 2009, in order to be considered in the selection of the second round candidates. Presentations and discussion topics of these sessions are also available at the Web site shown above.

Technical Evaluations of SHA-3 Candidates

NIST plans to hold a second round of review to evaluate the security of the submitted algorithms. In addition to the ongoing public review and evaluation, NIST will conduct computational efficiency tests on the candidate algorithms using various platforms. The public is also invited to conduct similar testing and to compare results. The rights to those candidates not selected for the second round of review will be returned to their owners. At the start of the second review period, submitters will have the option of providing updated optimized implementations for use during this phase of evaluation.

A second SHA-3 Candidate Conference will be held in the third quarter of 2010 to continue the review and evaluation of candidate algorithms and to reduce the number of candidate algorithms to approximately five. After another period to review these finalist candidates, NIST will hold a third SHA-3 Candidate Conference to discuss these candidates. NIST will then select the winning algorithm and document the technical rationale for the selection in a final report. A revision to the *Secure Hash Standard* will be proposed, including the newly selected SHA-3, for public review before final action to adopt the revised standard. NIST plans to support the standard by developing a program

to validate implementations of the new hash algorithm for conformance to the specifications.

The public competition for a new hash algorithm was modeled after the very successful Advanced Encryption Standard (AES) competition—a process that NIST had followed to develop the AES (FIPS 197). NIST launched the AES competition by first publishing the minimum requirements, submission requirements, and the evaluation criteria for public comment. An AES workshop was held to discuss these requirements and evaluation criteria before a call for new algorithms was issued. The review, analysis, and a variety of tests of the submitted algorithms were conducted in stages, by NIST and by the international cryptographic community. Public feedback was provided through an electronic forum and public conferences. After the winning algorithm was selected, NIST published a report that documented the AES development effort as well as the final selection.

Hash Forum

NIST has established a Hash Forum for discussion of the hash cryptographic algorithm project. A mailing list that distributes posted messages to the list members is available. Those who wish to be included on the mailing list (hash-forum@nist.gov) can find instructions for joining at http://csrc.nist.gov/groups/ST/hash/email_list.html.

Considerations in the Selection of SHA-3

SHA-3 is expected to offer features or properties that exceed, or improve upon, the SHA-2 family of algorithms specified in FIPS 180-3. The security strength of SHA-3 should be close to the theoretical maximum for the different required hash sizes, and for both the collision resistance and one-way properties. SHA-3 algorithms are expected to be designed to resist any potentially successful attacks on SHA-2 functions. In addition, SHA-3 should be implementable on a variety of platforms, and should be more efficient than the current hash algorithms.

NIST would prefer a single hash algorithm family that generates different message digest sizes in a similar manner. However, if more than one suitable candidate family is identified, and each provides significant advantages, NIST may consider recommending more than one family for inclusion in the revised *Secure Hash Standard*.

The hash algorithm will be publicly disclosed and available worldwide without royalties or any intellectual property restrictions. The algorithm will also be capable of being implemented on a wide range of hardware and software platforms, and support message digest sizes of 224, 256, 384, and 512 bits and a maximum message length of at least 2^{64}-1 bits.

Contact for Information about the Cryptographic Hash Project

Questions concerning the technical requirements for SHA-3 may be directed to:

Mr. William E. Burr
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
Telephone: 301-975-2914, Email: william.burr@nist.gov, Fax: 301-975-8670

Related Publications

The following FIPS and NIST Special Publications (SPs) require the use of a NIST-approved hash algorithm:

FIPS 186-2, *Digital Signature Standard*
FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*
NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs)*

For information about NIST standards and guidelines that are referenced in this bulletin, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

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.