An official website of the United States government Here's how you know

Hash Functions

PROJECT LINKS

Overview

News & Updates

Events

Publications

SHA-3 Project

A cryptographic hash algorithm (alternatively, hash "function") is designed to provide a random mapping from a string of binary data to a fixed-size “message digest” and achieve certain security properties. Hash algorithms can be used for digital signatures, message authentication codes, key derivation functions, pseudo random functions, and many other security applications. The Federal Information Processing Standard (FIPS 180-4), *Secure Hash Standard*, specifies seven cryptographic hash algorithms for Federal use, and is widely adopted by the information technology industry as well.

In 2004-2005, several cryptographic hash algorithms were successfully attacked, and serious attacks were published against the NIST-approved SHA-1. In response, NIST held two public workshops to assess the status of its approved hash algorithms, and to solicit public input on its cryptographic hash algorithm policy and standard. As a result of these workshops, NIST decided to develop a new cryptographic hash algorithm for standardization through a public competition. The new hash algorithm would be referred to as *SHA-3*.

NIST announced the SHA-3 Cryptographic Hash Algorithm Competition on November 2, 2007, and ended the competition on October 2, 2012, when it announced KECCAK as the winning algorithm to be standardized as the new SHA-3.

SHA-3 Competition (11/2/2007 – 10/2/2012)

- NISTIR 7620, *Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition*
- NISTIR 7764, *Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition*
- NISTIR 7896, *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition* (Final Report)

- Some documentation from the final KECCAK algorithm package:
  - The KECCAK reference, Version 3.0
  - The KECCAK SHA-3 submission, Version 3
  - Intellectual Property Statements
- The KECCAK designers maintain up-to-date information about Keccak at the KECCAK Team webpages.

SHA-3 Standardization (FIPS 180-4 and FIPS 202)

- FIPS 180-4, *Secure Hash Standard (SHS)*
- FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*

SHA-3-Derived Functions (SP 800-185)

- NIST SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*

Workshops/Conferences

- SHA-3 2014 Workshop (March 2014)
- Third SHA-3 Candidate Conference (March 2012)
- Second SHA-3 Candidate Conference (August 2010)
- First SHA-3 Candidate Conference (February 2009)
- Second Cryptographic Hash Workshop (August 2006)
- First Cryptographic Hash Workshop (October 2005)

The Internet Archive has an archive copy of NIST's SHA-3 Development site (as of August 29, 2017), including the submission packages (with the specification and implementations) of all candidate algorithms, public comments received, conference materials, etc.

ADDITIONAL PAGES

NIST Policy on Hash Functions

SHA-3 Project

SHA-3 Standardization

CONTACTS

Morris Dworkin
morris.dworkin@nist.gov

GROUP

Cryptographic Technology

TOPICS

Security and Privacy: secure hashing

RELATED PROJECTS

Cryptographic Standards and Guidelines
Digital Signatures

Created January 04, 2017, Updated September 16, 2026

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications?
Subscribe

Contact Us | Our Other Offices

Send inquiries to csrc-inquiry@nist.gov

Site Privacy | Accessibility | Privacy Program | Copyrights | Vulnerability Disclosure |

No Fear Act Policy | FOIA | Environmental Policy | Scientific Integrity |

Information Quality Standards | Commerce.gov | Science.gov | USA.gov | Vote.gov