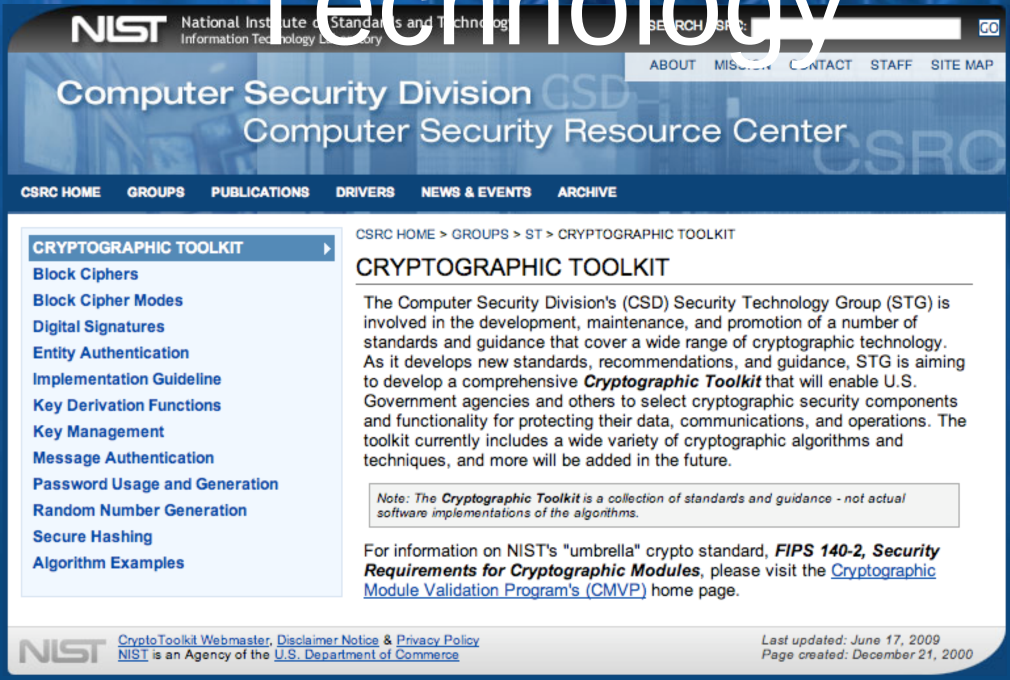
Cryptographic Technology



CRYPTOGRAPHIC TOOLKIT

The Computer Security Division's (CSD) Security Technology Group (STG) is involved in the development, maintenance, and promotion of a number of standards and guidance that cover a wide range of cryptographic technology. As it develops new standards, recommendations, and guidance, STG is aiming to develop a comprehensive ***Cryptographic Toolkit*** that will enable U.S. Government agencies and others to select cryptographic security components and functionality for protecting their data, communications, and operations. The toolkit currently includes a wide variety of cryptographic algorithms and techniques, and more will be added in the future.

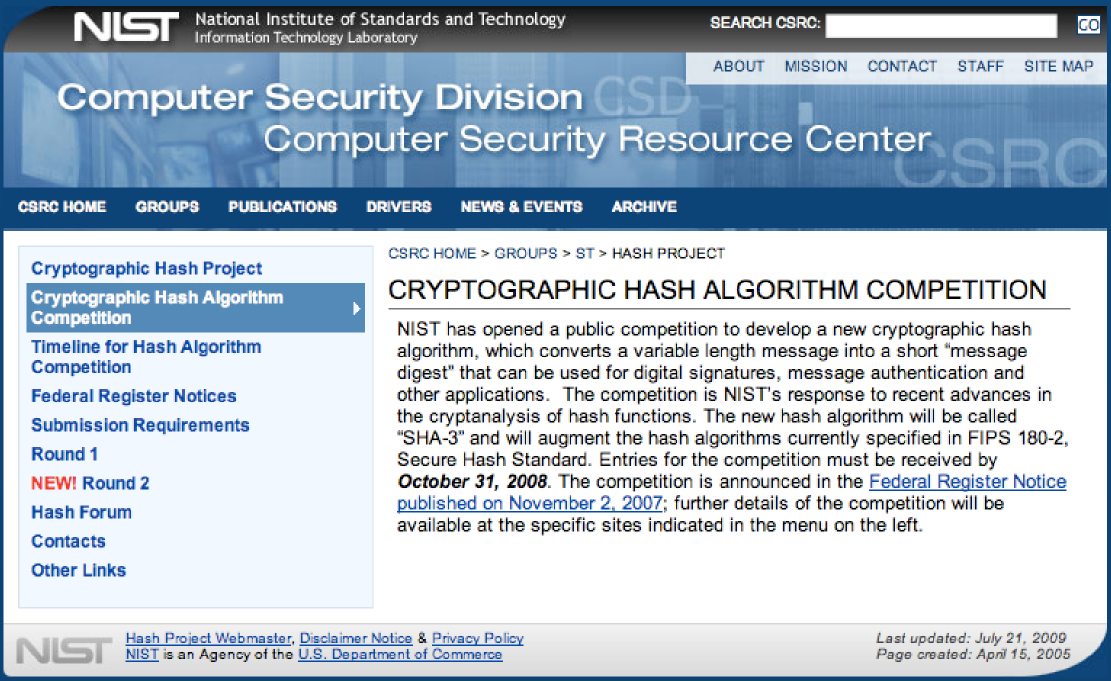
*Note: The **Cryptographic Toolkit** is a collection of standards and guidance - not actual software implementations of the algorithms.*

For information on NIST's "umbrella" crypto standard, ***FIPS 140-2, Security Requirements for Cryptographic Modules***, please visit the Cryptographic Module Validation Program's (CMVP) home page.

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

Last updated: June 17, 2009
Page created: December 21, 2000

http://csrc.nist.gov/CryptoToolkit


NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
ABOUT
MISSION
CONTACT
STAFF
SITE MAP
Computer Security Division CSD
Computer Security Resource Center CSRC
CSRC HOME
GROUPS
PUBLICATIONS
DRIVERS
NEWS & EVENTS
ARCHIVE
Cryptographic Hash Project
Cryptographic Hash Algorithm Competition
Timeline for Hash Algorithm Competition
Federal Register Notices
Submission Requirements
Round 1
NEW! Round 2
Hash Forum
Contacts
Other Links
CSRC HOME > GROUPS > ST > HASH PROJECT

CRYPTOGRAPHIC HASH ALGORITHM COMPETITION

NIST has opened a public competition to develop a new cryptographic hash algorithm, which converts a variable length message into a short "message digest" that can be used for digital signatures, message authentication and other applications. The competition is NIST's response to recent advances in the cryptanalysis of hash functions. The new hash algorithm will be called "SHA-3" and will augment the hash algorithms currently specified in FIPS 180-2, Secure Hash Standard. Entries for the competition must be received by ***October 31, 2008***. The competition is announced in the Federal Register Notice published on November 2, 2007; further details of the competition will be available at the specific sites indicated in the menu on the left.

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

Last updated: July 21, 2009
Page created: April 15, 2005

http://www.nist.gov/hash-function

NIST
National Institute of Standards and Technology

Selected Publications

- Block Ciphers
  - FIPS 197, Advanced Encryption Standard (AES)
  - Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- Block Cipher Modes of Operation
  - Special Publication 800-38A-D, Specifies Five Confidentiality Modes (ECB, CBC, CFB, OFB, and Counter), CMAC Mode for Authentication, CCM Mode for Authentication and Confidentiality, and GCM and GMAC Modes
- Digital Signatures
  - FIPS 186-3, Digital Signature Standard (DSS) – including DSA, ECDSA, and RSA
  - Special Publication 800-102, Recommendation for Digital Signature Timeliness
  - Special Publication 800-106, Randomized Hashing for Digital Signatures
- Entity Authentication
  - FIPS 196 – Entity Authentication Using Public Key Cryptography
- Implementation Guideline
  - Special Publication 800-21-1, Second Edition, Guideline for Implementing Cryptography in the Federal Government
- Key Derivation Functions
  - Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions
- Key Management
  - Special Publication 800-57 Parts 1-3, Recommendation for Key Management – Part 1: General; Part 2: Best Practices for Key Management Organizations; and Part 3: Application-Specific Key Management Guidance
  - Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
  - Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
- Message Authentication
  - FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC)
- Random Number Generation
  - Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)
- Secure Hashing
  - FIPS 180-3, Secure Hash Standard
  - Special Publication 800-107, Recommendation for Using Approved Hash Algorithms

Additional Information: http://csrc.nist.gov

NIST
National Institute of
Standards and Technology