Hash Competition

Timeline

- ✓01/23/07 Draft submission criteria published
- ✓11/02/07 Federal Register announcement of SHA-3 Competition
- ✓08/31/08 Preliminary submissions due
- ✓10/31/08 Submissions due – 64 received
- ✓12/09/08 Announced 51 First round candidates
- ✓02/25/09 First SHA-3 Candidate Conference, Leuven Belgium
- ✓07/24/09 Announced 14 second round candidates
- ✓09/15/09 Tweaks accepted, second round began
- ➢3Q10 Second SHA-3 Candidate Conference, UCSB
- ➢4Q10 Announce finalist candidates
- ➢1Q11 Final tweaks of candidates
- ➢1Q12 Last SHA-3 Candidate Conference
- ➢2Q12 Announce winner
- ➢4Q12 FIPS package to Secretary of Commerce

Second Round Candidates

- Blake
  - –Swiss, HAIFA
- Blue Midnight Wish
  - –Norway, WideP MD
- CubeHash
  - –US, Sponge variant
- ECHO
  - –France, HAIFA
- Fugue
  - –US, Sponge variant
- Grøstl
  - –European, WideP MD
- HAMSI
  - –Turkey, MD
- JH
  - –Singapore, novel construction
- Keccak
  - –European, Sponge
- LUFFA
  - –Japan, Sponge variant
- SHABAL
  - –France, WideP MD
- SHAvite-3
  - –Israel, HAIFA
- SIMD
  - –France, WideP MD
- SKEIN
  - –US, Matyas-Meyer-Oseas construction

NIST
National Institute of Standards and Technology
U.S. Department of Commerce