Proposed Timeline for the Development of New Hash Functions

Elaine Barker
NIST
ebarker@nist.gov
301-975-2911

Prior to a Competition

- **Aug. 2006 Second Hash Function Status and Research Workshop:**
  - Assess current status
  - Discuss hash function development strategy
  - Encourage further research.
- **2007 Third Hash Function Workshop 2007**
- **Decision**: NIST will decide whether or not to hold additional workshops on hash function research, especially on requirements and evaluation criteria, before initiating the competition.

Timeline for the Competition

Year 1 (2008?)

- 1Q: Draft and publish the minimum acceptability requirements, evaluation criteria, and submission requirements for public comments. Announce a public workshop to discuss these requirements.
- 2Q: Public comment period ends.
- 2Q: Host a workshop to discuss the requirements.
- 3Q: Finalize and publish the minimum acceptability requirements, evaluation criteria and submission requirements. Request submissions for new hash functions.

Year 2 (2009?)

- 2Q: Review submitted algorithms, and select candidates that meet basic submission requirements.
- 3Q: Host the First Hash Function Candidate Conference. Announce first round candidates.
- 3Q: Call for public comments on the first round candidates.

Year 3 (2010?)

- 1Q: Hold the Second Hash Function Candidate Conference. Discuss analysis results on the first round candidates.
- 2Q: Public comment period on the first round candidates ends.
- 3Q: Address public comments; select the second round finalists. Prepare a report to explain the selection.
- 3Q: Announce the second round finalists. Publish the selection report, and call for public comments on the second round candidates.

Year 4 (2011?)

- 2Q: Host the Third Hash Function Candidate Conference. Submitters of the second round finalists discuss comments on their algorithms.
- 2Q: Public comment period ends.
- 3Q: Address public comments, and select the finalist. Prepare a report to describe the final selection(s).
- 4Q: Announce the new hash function(s).

Year 5 (2012?)

- 1Q: Publish a draft standard for public comments.
- 2Q: Public comment period ends.
- 3Q: Address public comments.
- 4Q: Publish the new hash function standard.