The Second Cryptographic Hash Workshop
Santa Barbara, CA
August 24-25, 2006 (Starting at 1PM, August 24)
Submission deadline: May 12, 2006 (Workshop without proceedings)

In response to the SHA-1 vulnerability that was announced in Feb. 2005, NIST held a Cryptographic Hash Workshop on Oct. 31-Nov. 1, 2005 to solicit public input on its cryptographic hash function policy and standards. NIST continues to recommend a transition from SHA-1 to the larger approved hash functions (SHA-224, SHA-256, SHA-384, and SHA-512). In response to the workshop, NIST has also decided that it would be prudent in the long-term to develop an additional hash function through a public competition, similar to the development process for the block cipher in the Advanced Encryption Standard (AES).

Before initiating the competition, NIST plans to host several more public workshops that will focus on hash function research. The next workshop will be held on August 24-25, 2006, in conjunction with Crypto 2006, with the following goals:

- Explore potential mathematical principles and structures that can provide the foundation for cryptographic hash functions;
- Foster accelerated research on the analysis of hash functions, especially the SHA-2 hash functions;
- Survey the uses of hash functions, and investigate the properties that are assumed, used, or needed. Identify and articulate the required or desirable properties for future hash functions.

NIST solicits research, surveys, discussion papers, presentations, case studies, panel proposals, and participation from all interested parties, including researchers, system architects, vendors, and users. NIST will post the accepted papers and presentations on the workshop web site and include these in a workshop handout. However, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere. To avoid the possible duplication of papers accepted for this workshop and Crypto 2006, submissions will NOT be considered for this workshop if they are substantially similar to the submissions accepted for Crypto 2006. Topics for submissions should include, but are not limited to, the following:

Mathematical Foundations
- Iterative structures, i.e., Damgård-Merkle or alternatives;
- Compression function constructions, e.g. Davies-Meyer;
- Hashing modes, e.g. randomized hashing or keyed hashing;
- Formal properties.

Analysis and Design
- Analysis and design of hash functions and their components;
- New cryptanalytic techniques against hash functions;
- Security report on existing hash functions, especially SHA-2;
- Tools for designing and analyzing compression functions;
- Provable properties of compression functions, e.g., reductions to hard problems.

Practical Uses and Pitfalls
- Uses of hash functions in applications and protocols;
- Properties of hash functions that are assumed, required, or obtained in practice;
- Vulnerabilities of hash functions caused by unexpected properties or misuse;
- Desirable properties for future hash functions.

Deadlines:

- **Submission Deadline: May 12, 2006**
- **Authors Notified: June 23, 2006**
- **Workshop Handout Version Deadline: July 21, 2006**

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). Paper submissions must not exceed 15 pages (single space, two column format with 1" margins using a 10 pt or larger font) and have no header or footer text (e.g., no page numbers). Proposals for presentations or panels should be no longer than five pages; panel proposals should include possible panelists and an indication of which panelists have confirmed their participation.

Please submit the following information to **hash-function@nist.gov**

- Name, affiliation, email, phone, postal address for the primary contact author
- First name, last name, and affiliation of each co-author
- The finished paper, presentation, or panel proposal in PDF format as an attachment.

All submissions will be acknowledged.

General information about the workshop including the registration and accommodation information will be available at the workshop website: **http://www.nist.gov/hash-function**