NIST Hash Function Update

John Kelsey, NIST

NOTE: See following URL for reliable info

If my slides disagree with website, trust website

http://csrc.nist.gov/groups/ST/hash/

Very Approximate Timetable

- **2008: Get Submissions**
  - **Aug 30 deadline for us to check submissions**
  - **Oct 31 deadline for submission**
- **2009: Start with submissions**
  - **Announce candidates, hold first AHS workshop***
- 2010: Select and announce finalists
  - Announce finalists, hold next AHS workshop
  - *Accept tweaks*
- *2011: Keep analyzing, maybe insert a year*
  - *Analyze what's left*
- *2012: Announce a winner?*

What We Want from a New Hash

- Secure
- Simple enough to analyze/understand
- Fits into existing slots for approved hashes
  - DSA, RNG, KDF, HMAC
  - Output sizes: 224, 256, 384, 512
- Good performance

http://csrc.nist.gov/groups/ST/hash/

Advertisement

- We are looking for a guest researcher with in-depth knowledge of hash functions
- Interesting work, not much money
- If you’re interested see me here or e-mail me at john.kelsey at nist.gov

http://csrc.nist.gov/groups/ST/hash/

Questions (Bidirectional)

- How many submissions will come from people in this room?
- How many submissions will we get

- Any concerns from people here?