Hash Workshop Wrapup

Agreement

- Don’t really know what we are doing
  - AES competition was a learning experience
  - Big safety margin
- Different apps: different requirements
  - Collision resistance, one-way, PRF…
- Parameterize number of rounds
  - But don’t give users too much choice
- Variable size is good too
- Need hash function modes standards
- NIST should favor security over performance
  - But we’re better at measuring performance
- Only 1 hash standard (or 2, see next slide)

Disagreement

- Salted hash function
  - Cryptographers: good idea
  - Implementers: No way in *!##, salted modes
- Separate on-line & in-memory stds
  - Cryptographers: most seem to like
  - Implement: don’t need/wouldn’t use in-mem
- “ad hoc” vs “hard problem”
  - Probably secure? Provably secure?

A few Other Ideas

- Should allow bigger changes to finalists
  - In AES comp. little change after finalist selection
    - IP issues? Can candidates steal from each other?
- Grants for analysis
  - Who (besides NIST) would pay?
- Need mandatory to implement hash robustness in protocols
  - Concatenate 2 different hashes?

Way Forward

- Workshop largely on requirements, criteria and ground-rules
  - Where and when
- AES-like competition