NIST Update
Crypto 2013 Rump Session

John Kelsey, NIST

See http://csrc.nist.gov/ for more details.

Hash Workshop 2014

- NIST is having another hash workshop
- Colocated with Crypto 2014
  - Friday and Saturday
- Submission deadline April 12, 2014

All things SHA2 or SHA3 including

Cryptanalysis	**Performance**	**Side-channels**
Small Perms	**Variant Modes**	**Tree hashing**

http://csrc.nist.gov/groups/ST/hash/sha-3/Aug2014/index.html
http://csrc.nist.gov/groups/ST/hash/sha-3/

NIST Beacon

- **Experimental** online service providing signed **public** random numbers
  - One random number per minute
  - Hash chained, signed, sequence-numbered
  - Whole sequence published and available online

- Down for a month or so.
- Should be back up Real Soon Now
- Trying to get cert from federal CA.

https://beacon.nist.gov/home
http://www.nist.gov/itl/csd/ct/nist_beacon.cfm

Current/Recent Publications

- SP 800-38G: **Format Preserving Encryption**
  - Public comment period closes **Sept 3, 2013**

- FIPS 186-4: **Digital Signature Standard**
  - Recently published (similar to 186-3)
  - DSA, ECDSA, RSA signatures
- SP 800-130: **Key Management Framework**
  - Recently published
- SP 800-56A: **Discrete Log Key Agreement**
  - Recently revised

See http://csrc.nist.gov/publications/

Thank-you!

- Hash Workshop 2014

http://csrc.nist.gov/groups/ST/hash/sha-3/

- NIST Beacon

http://www.nist.gov/itl/csd/ct/nist_beacon.cfm

- Recent and Upcoming Publications

http://csrc.nist.gov/