Recommended reading (protocols)

- Defending Against Redirect Attacks in Mobile IP
  - Deng, Zhou, Bao (Labs for Information Technology, Singapore)
  - Review of two security issues in routing optimization for Mobile IP, new protocol design
  - Link provided in the IS

Starting new thread...

- Yet one more lecture on protocols to come (in two weeks, Oct. 25)
- No in-class lecture next week
- New tread – assignment (to come) on AES
  - Bits of background info follows, more in the IS and next week in the assignment

Advanced Encryption Standard Exercise

- Rumors from NIST in 1996
- January 1997 – Official announcement
- September 1997 – Call for Proposals
- August 1998 – 15 candidates announced
- August 1999 – 5 finalists
- 2 October 2000 – Choice of algorithm
- Late 2000, early 2001 – First implementations (PGP 7.0.3)
- Spring 2001 – Standard – FIPS

AES finalists

- MARS (IBM)
  - high security, large ROM req., no good HW impl.
- RC6 (RSA Labs)
  - adequate security, moderate ROM req., average HW impl.
- Rijndael (Rijmnen, Daemen – Belgium!)
  - adequate security, fast-SW, low memory req., fast-HW
- Serpent (Anderson, Biham, Knudsen)
  - high security, low memory req., slow-SW, fast-HW
- Twofish (Schneier et al.)
  - adequate security, high ROM req., average HW impl.

AES-Rijndael

- Input & Output: 128 bits
- Key: 128, 192 or 256 bits
- Processing by bytes – basic units
- Operations – addition (XOR), multiplication
- 10, 12 or 14 rounds (given by key length)
  - Initial Round Key addition
  - Last Round slightly different

AES-Rijndael (cont'd)

- PDF slides from the algorithm authors

http://csrc.nist.gov/CryptoToolkit/aes/rijndael/misc/nissc2.pdf

- Neat Rijndael animation…

http://www.esat.kuleuven.ac.be/~rijmen/rijndael/Rijndael_Anim.zip