A call for stream ciphers by ECRYPT

Bart Preneel
COSIC, K.U.Leuven, Belgium
ecrypt-contact@ecrypt.eu.org

http://www.ecrypt.eu.org

ECRYPT

- European Network of Excellence in Cryptology and Watermarking
- EU FP6-IST programme
- February 2004 - January 2008
- Total budget: 8.4 M€ (EC contribution: 5.6 M€)
- 32 partners, 14 countries, 250 researchers

- symmetric key: Matt Robshaw, Royal Holloway

http://www.ecrypt.eu.org/stream

Stream ciphers: requirements

- security equivalent to AES
- ideally free to use
- resynchronization mechanism
- offer authenticated encryption
- better performance than block ciphers in software or hardware:
  - either high speed (< 7 cycles/byte)
  - or very compact (< 1000 gates)
- tunable security

http://www.ecrypt.eu.org/stream

ECRYPT "Competition" Requirements:

- Profile 1: high performance in software (32/64-bit):
  - must support 128-bit key, 64 and 128-bit IVs
  - total number of key stream bits: 2^{96}
- Profile 2: low footprint:
  - must support 80-bit key, 32-bit and 64-bit IVs
  - total number of key stream bits: 2^{64}
- Profile 1A and 2A: authenticated encryption
- mandatory: IV for resynchronization

http://www.ecrypt.eu.org/stream

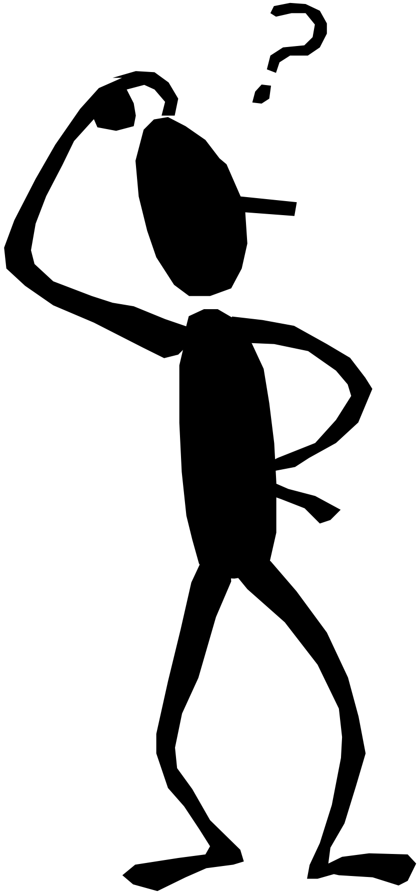
Principles

- formal submission requirements limited
- not a formal competition but rather “pool of algorithms” evaluated by broader community
- merge and design tuning allowed after 15 months
- successful if goals achieved: input to standardization (ECRYPT is not a standardization body)

Timing

- Formal announcement: December 2004
- Submissions due: April 29 2005
- Stream cipher workshop: May 26-27 2005
- End of phase 1: February 2006
- Beginning of phase 2: July 2006
- End of phase 2: September 2007
- Final report: January 2008

The end



Thank you for your attention

http://www.ecrypt.eu.org/stream