Lecture 10:
Two Fish on the Rijndael

The algorithm might look haphazard, but we did everything for a reason. Nothing is in Twofish by chance. Anything in the algorithm that we couldn't justify, we removed. The result is a lean, mean algorithm that is strong and conceptually simple.

Bruce Schneier

CS588: Cryptography
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/evans

Menu

- Why Cryptographers should talk to laywers?
  - Clipper
  - DMCA
- AES Candidates
  - RC6
  - Blowfish
- AES Winner - Rijndael

Why Cryptographers should talk to laywers (1994)

- 1993 – AT&T markets secure telephony device
- Law enforcement: US courts can authorize wire taps, must be able to decrypt
- NSA proposes Clipper Chip
  - Secret algorithm (Skipjack), only implemented in hardware