Lecture 5: One Fish, Two Fish, Blowfish, Blue Fish

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

CS551: Security and Privacy
University of Virginia
Computer Science

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

Menu

- Clipper
- AES Program
- AES Candidates
  - RC6
  - Blowfish

Problem Set 1