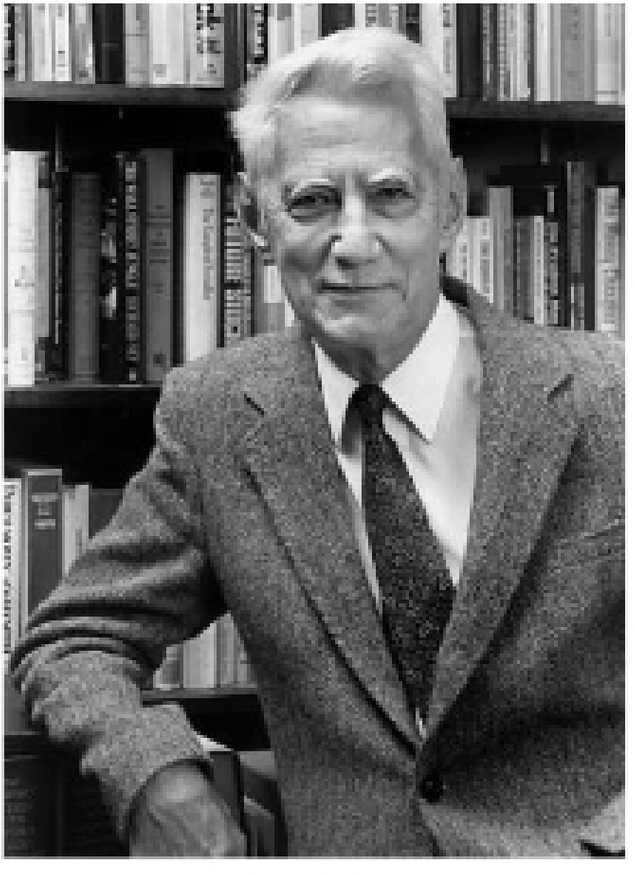
Lecture 2: Perfect Ciphers (in Theory, not Practice)

Shannon was the person who saw that the binary digit was the fundamental element in all of communication. That was really his discovery, and from it the whole communications revolution has sprung.
R G Gallager

I just wondered how things were put together.
Claude Shannon



Claude Shannon,
1916-2001

CS588: Cryptology
University of Virginia
Computer Science

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

Menu

- Survey Results
- Perfect Ciphers
- Entropy and Unicity

Survey Responses

- Majors: Cognitive Science, Computer Science (13), Computer Engineering (2), Economics, Math
- Year: Third year: 6, Fourth Year: 10, Grad: 1, 2005: 1
- Midterm: **March 3: 12**, March 15: 3, March 17: 2, March 22: 1
- Broken in?: No: 13, Yes: 5

Full answers are on the course web site