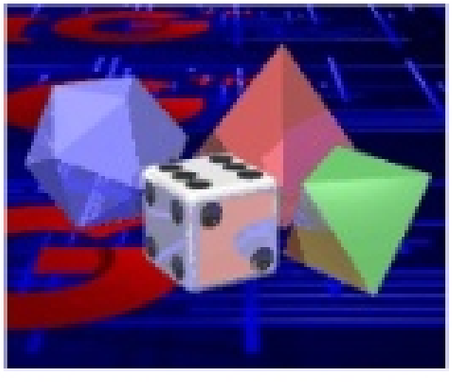
Lecture 14:
Digital Cash, Randomness



CS588: Security and Privacy
University of Virginia
Computer Science

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

Menu

- Randomness
- Cannibalistic Voting Protocols
- Digital Cash

Random Numbers

For numbers in range $0...2^{n-1}$, an observer with the first m - 1 numbers, cannot guess the m^{th} with probability better than $1/2^{n}$.