

Applied Cryptography

Lecture 0

Manoj Prabhakaran

University of Illinois Urbana-Champaign

What is Cryptography?

What is Cryptography?

- It's all about controlling access to information



What is Cryptography?

- ⦿ It's all about **controlling** access to information
- ⦿ Access to learning and/or influencing information



What is Cryptography?

- ⦿ It's all about **controlling access to information**
- ⦿ Access to learning and/or influencing information
- ⦿ Do we know what we are talking about?



What is information?

What is information?

- ⦿ Or rather the lack of it?

What is information?

- ⦿ Or rather the lack of it?
- ⦿ Uncertainty

What is information?

- ⦿ Or rather the lack of it?
- ⦿ Uncertainty
- ⦿ The word is Entropy

What is information?

- ⦿ Or rather the lack of it?
- ⦿ Uncertainty
- ⦿ The word is Entropy
- ⦿ Borrowed from thermodynamics

What is information?

Rudolf Clausius



- ➊ Or rather the lack of it?
- ➋ Uncertainty
- ➌ The word is Entropy
- ➍ Borrowed from thermodynamics

What is information?

- ⦿ Or rather the lack of it?
- ⦿ Uncertainty
- ⦿ The word is Entropy
- ⦿ Borrowed from thermodynamics



Rudolf Clausius



Ludwig Boltzmann

What is information?

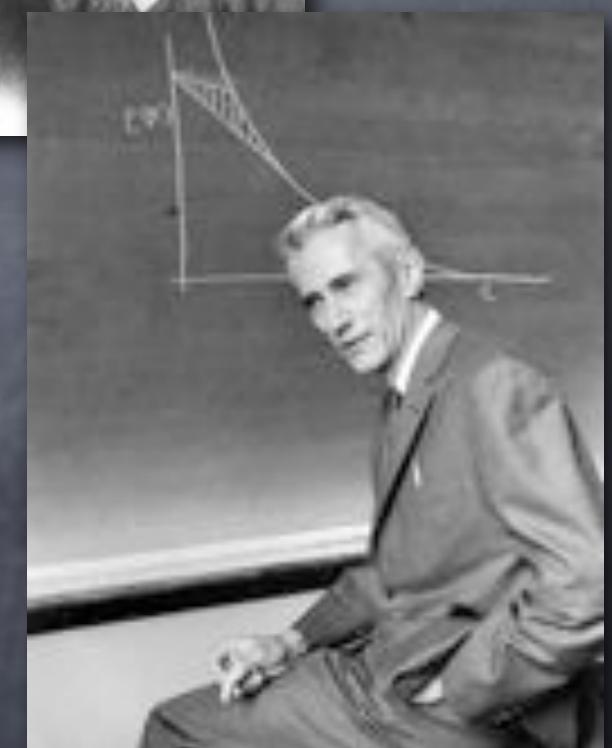
- ⦿ Or rather the lack of it?
- ⦿ Uncertainty
- ⦿ The word is Entropy
- ⦿ Borrowed from thermodynamics



Rudolf Clausius



Ludwig Boltzmann



Claude Shannon

What is information?

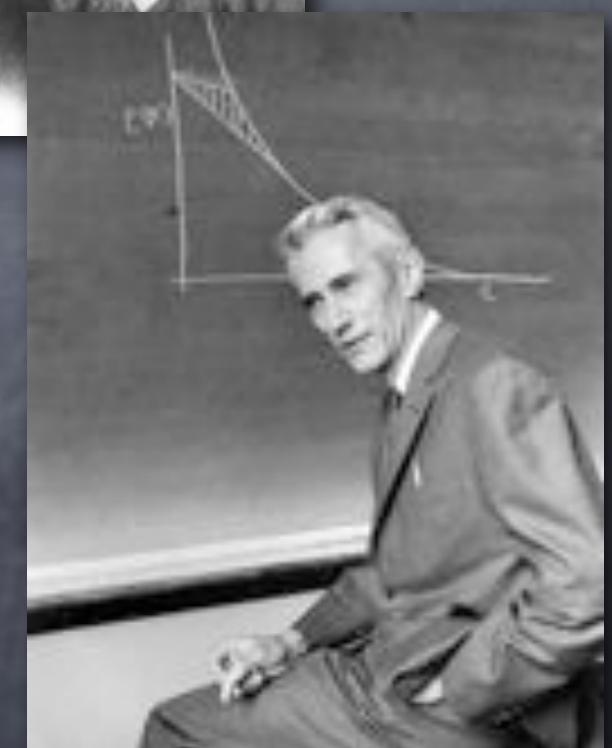
- ⦿ Or rather the lack of it?
- ⦿ Uncertainty
- ⦿ The word is Entropy
 - ⦿ Borrowed from thermodynamics
 - ⦿ An inherently “probabilistic” notion



Rudolf Clausius



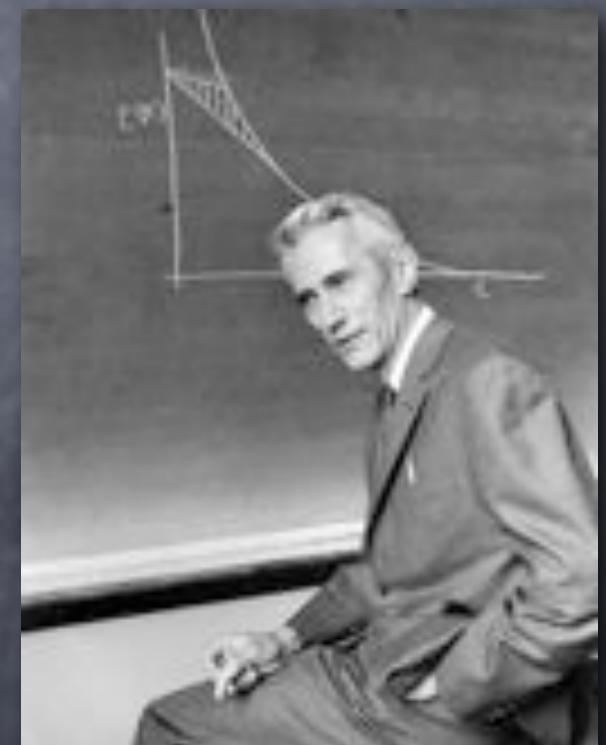
Ludwig Boltzmann



Claude Shannon

What is information?

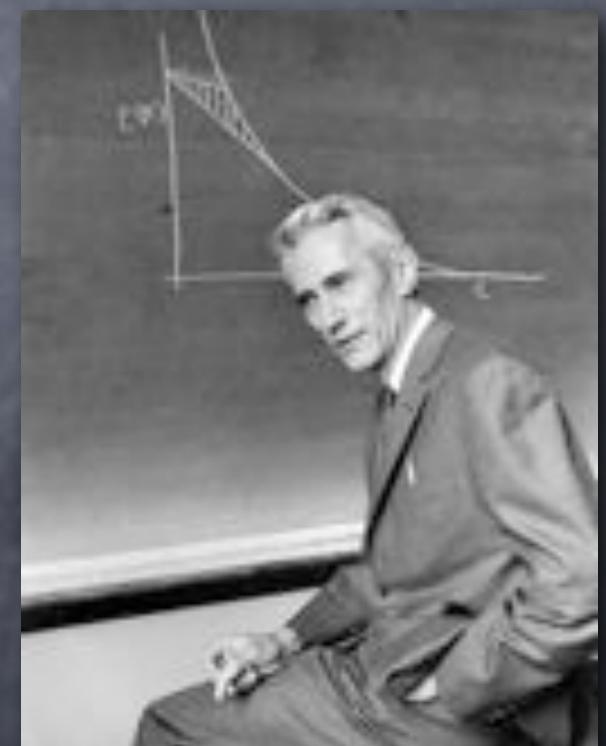
Claude Shannon



What is information?

- Information Theory: ways to quantify information

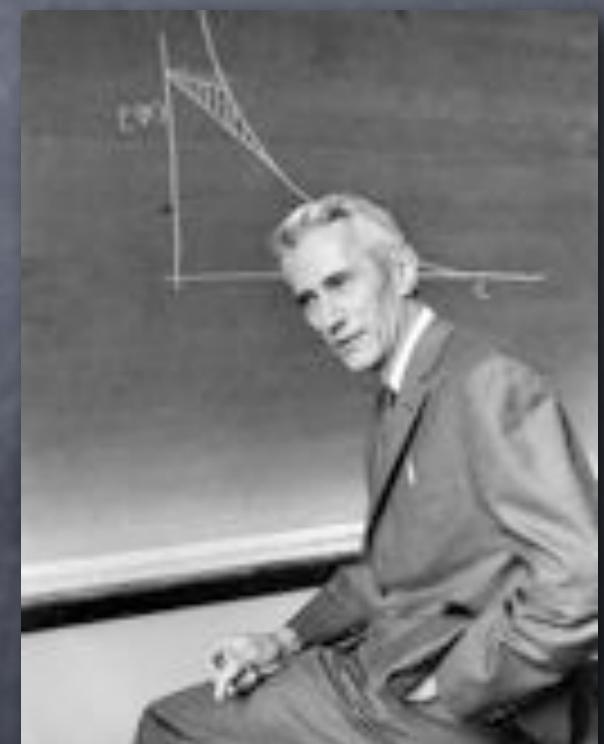
Claude Shannon



What is information?

- Information Theory: ways to quantify information
- Application 1: to study efficiency of communication (compression, error-correction)

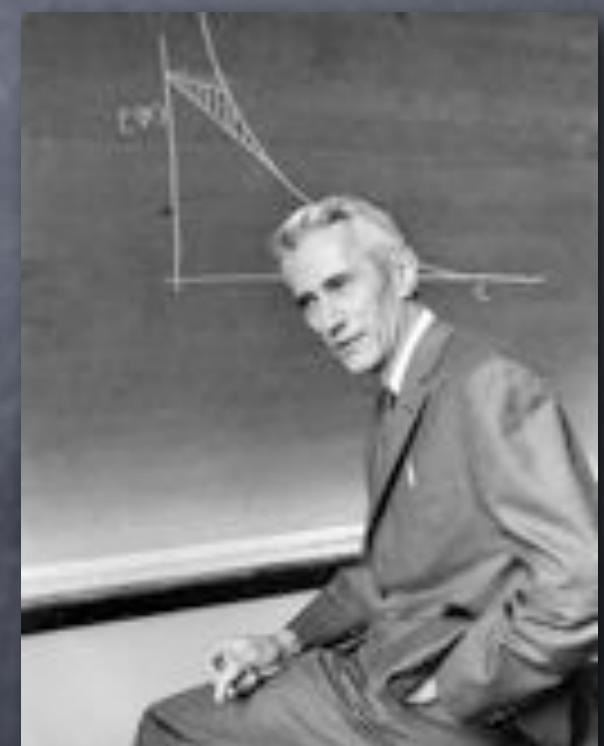
Claude Shannon



What is information?

- Information Theory: ways to quantify information
- Application 1: to study efficiency of communication (compression, error-correction)
- Application 2: to study the possibility of secret communication

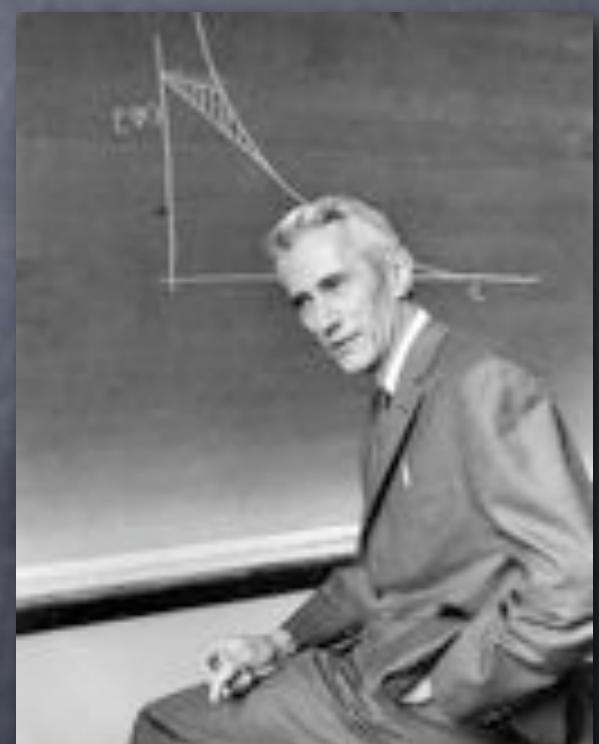
Claude Shannon



What is information?

- Information Theory: ways to quantify information
- Application 1: to study efficiency of communication (compression, error-correction)
- Application 2: to study the possibility of secret communication
 - The latter turned out to be a relatively easy question! Secret communication possible only if (an equally long) secret key is shared ahead of time

Claude Shannon



Access to Information

Access to Information

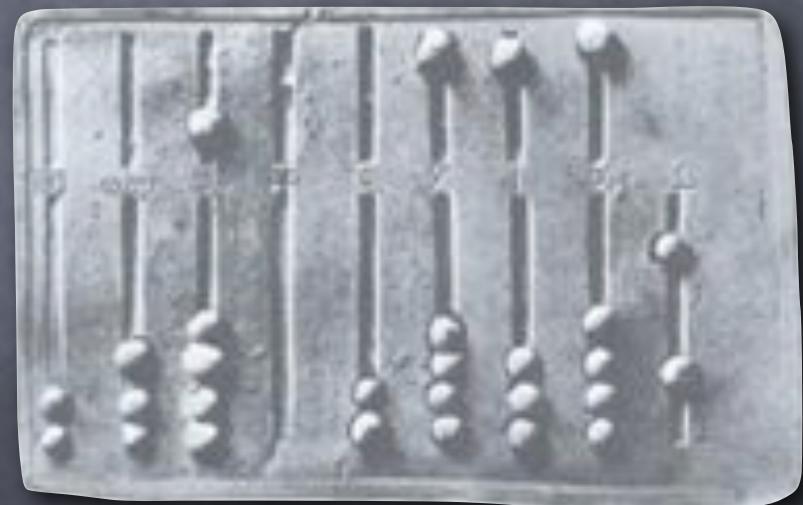
- A second look

Access to Information

- ⦿ A second look
- ⦿ Information at hand may still not be “accessible” if it is hard to work with it

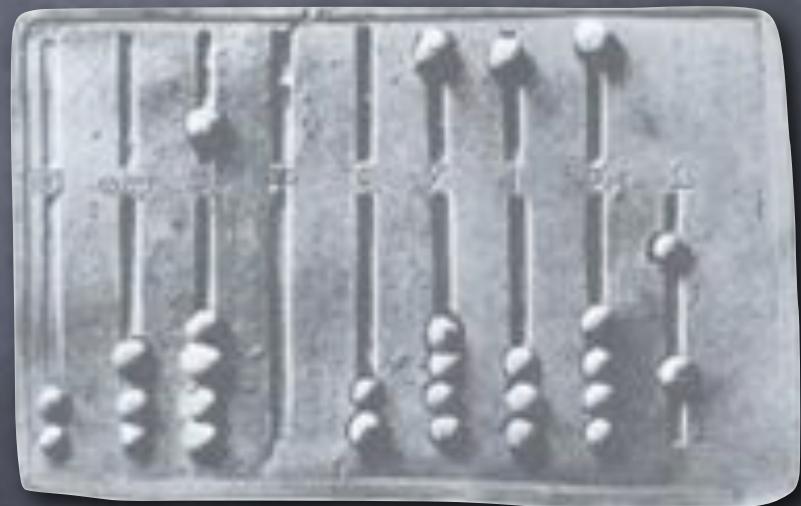
Access to Information

- ⦿ A second look
- ⦿ Information at hand may still not be “accessible” if it is hard to work with it
- ⦿ Computation!



Access to Information

- ⦿ A second look
- ⦿ Information at hand may still not be “accessible” if it is hard to work with it
- ⦿ Computation!
- ⦿ Shannon’s information may reduce uncertainty only for computationally all-powerful parties



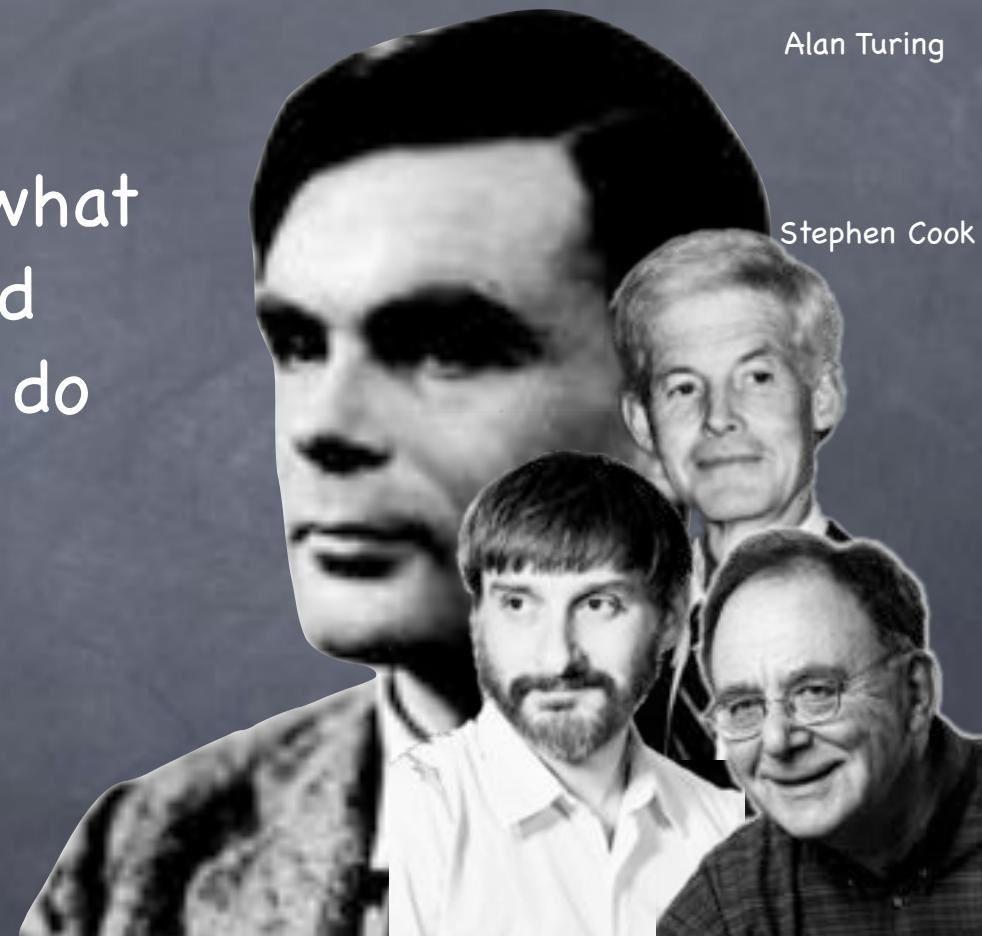
Computational Complexity

Computational Complexity

- A systematic study of what computationally bounded parties can and cannot do

Computational Complexity

- ⦿ A systematic study of what computationally bounded parties can and cannot do
- ⦿ A young and rich field



Alan Turing

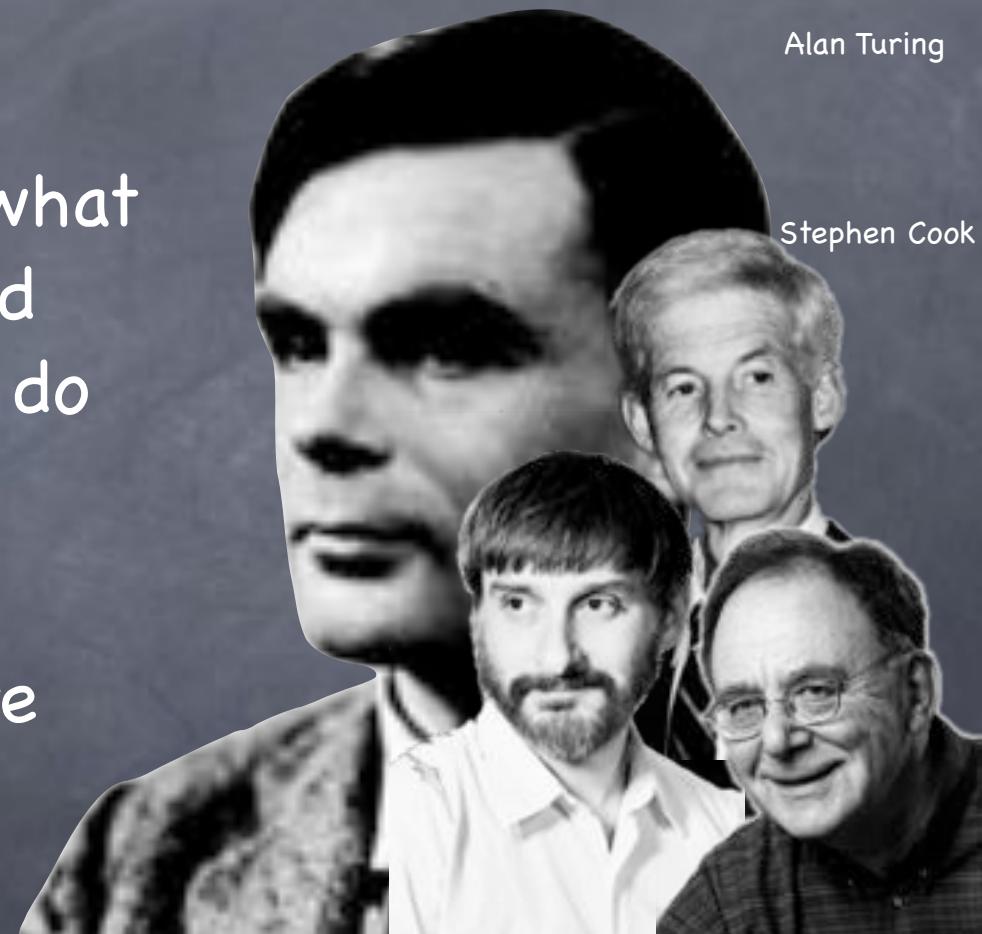
Stephen Cook

Leonid Levin

Richard Karp

Computational Complexity

- ⦿ A systematic study of what computationally bounded parties can and cannot do
- ⦿ A young and rich field
- ⦿ Much known, much more unknown



Alan Turing

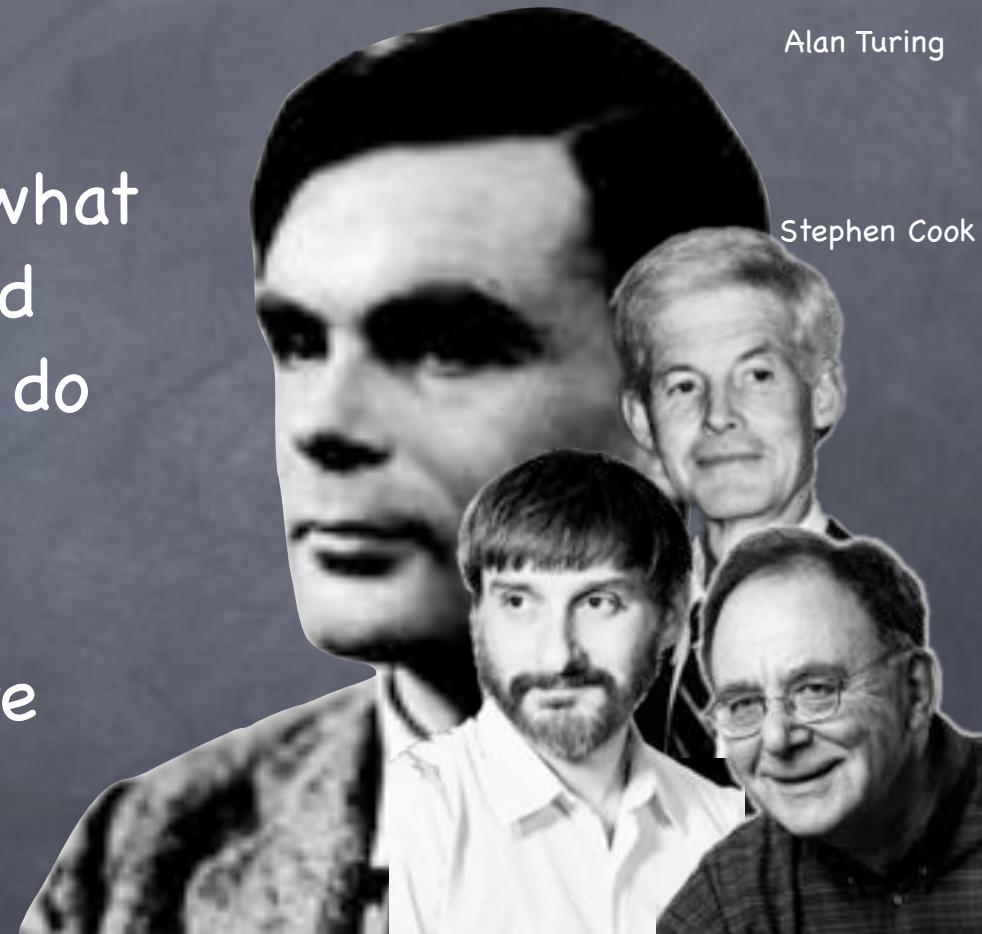
Stephen Cook

Leonid Levin

Richard Karp

Computational Complexity

- ⦿ A systematic study of what computationally bounded parties can and cannot do
- ⦿ A young and rich field
- ⦿ Much known, much more unknown
- ⦿ Much “believed”



Alan Turing

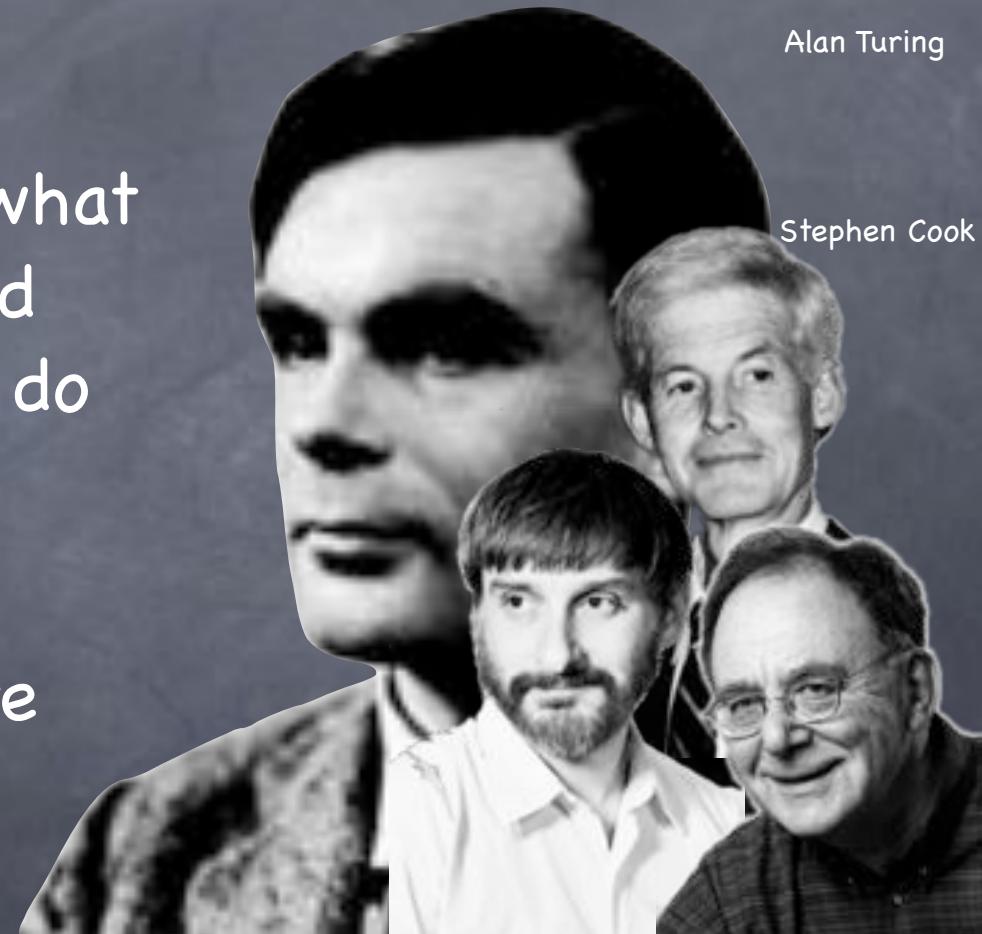
Stephen Cook

Leonid Levin

Richard Karp

Computational Complexity

- ⦿ A systematic study of what computationally bounded parties can and cannot do
- ⦿ A young and rich field
- ⦿ Much known, much more unknown
- ⦿ Much “believed”
- ⦿ Basis of the Modern Theory of Cryptography



Alan Turing

Stephen Cook

Leonid Levin

Richard Karp

Compressed Secret-Keys

Compressed Secret-Keys

- ⦿ Pseudo-random number generator

Compressed Secret-Keys

- ⦿ Pseudo-random number generator
- ⦿ a.k.a Stream Cipher

Compressed Secret-Keys

- ⦿ Pseudo-random number generator
 - ⦿ a.k.a Stream Cipher
 - ⦿ Generate a long string of random-looking bits from a short random seed

Compressed Secret-Keys

- ⦿ Pseudo-random number generator
 - ⦿ a.k.a Stream Cipher
 - ⦿ Generate a long string of random-looking bits from a short random seed



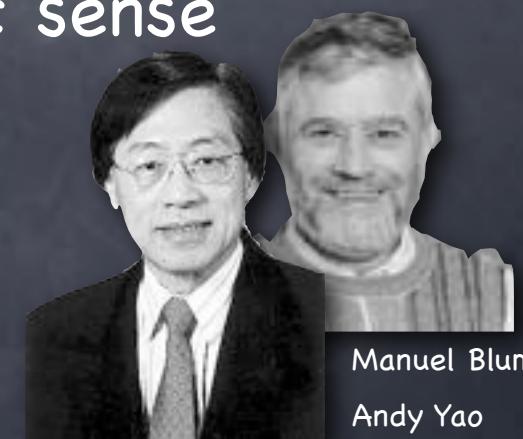
Compressed Secret-Keys

- ⦿ Pseudo-random number generator
 - ⦿ a.k.a Stream Cipher
 - ⦿ Generate a long string of random-looking bits from a short random seed
- ⦿ Impossible in the information-theoretic sense



Compressed Secret-Keys

- ⦿ Pseudo-random number generator
 - ⦿ a.k.a Stream Cipher
 - ⦿ Generate a long string of random-looking bits from a short random seed
- ⦿ Impossible in the information-theoretic sense
 - ⦿ But possible against computationally bounded players!



Manuel Blum
Andy Yao

The Public-Key Revolution

The Public-Key Revolution

- “Non-Secret Encryption”

The Public-Key Revolution

- “Non-Secret Encryption”
- No *a priori* shared secrets

The Public-Key Revolution

- “Non-Secret Encryption”
 - No a priori shared secrets
 - Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!

The Public-Key Revolution

- “Non-Secret Encryption”
- No a priori shared secrets
- Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!



The Public-Key Revolution



James Ellis

- ⦿ “Non-Secret Encryption”
- ⦿ No a priori shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!

The Public-Key Revolution

- ⦿ “Non-Secret Encryption”
- ⦿ No a priori shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!



James Ellis

Clifford Cocks

The Public-Key Revolution



James Ellis

Clifford Cocks

- ⦿ “Non-Secret Encryption”
- ⦿ No *a priori* shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!

The Public-Key Revolution

Malcolm Williamson



James Ellis

Clifford Cocks

- ⦿ “Non-Secret Encryption”
- ⦿ No a priori shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!
- ⦿ Publicly verifiable digital signatures

The Public-Key Revolution

- ⦿ “Non-Secret Encryption”
- ⦿ No a priori shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!
- ⦿ Publicly verifiable digital signatures



James Ellis



Merkle, Hellman, Diffie

Malcolm Williamson



Clifford Cocks

The Public-Key Revolution

- ⦿ “Non-Secret Encryption”
- ⦿ No a priori shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!
- ⦿ Publicly verifiable digital signatures



James Ellis

Malcolm Williamson



Clifford Cocks



Merkle, Hellman, Diffie



Shamir, Rivest, Adleman

The Public-Key Revolution

- ⦿ “Non-Secret Encryption”
- ⦿ No a priori shared secrets
- ⦿ Instead, a public key. Anyone can create encryptions, only the creator of the key can decrypt!
- ⦿ Publicly verifiable digital signatures
- ⦿ Forms the backbone of today’s secure communication



James Ellis

Malcolm Williamson



Clifford Cocks



Merkle, Hellman, Diffie



Shamir, Rivest, Adleman

Crypto-Mania

Crypto-Mania

- Public-Key cryptography and beyond!

Crypto-Mania

- ⦿ Public-Key cryptography and beyond!
- ⦿ Secret computation: collaboration among mutually distrusting parties

Crypto-Mania

- ⦿ Public-Key cryptography and beyond!
- ⦿ Secret computation: collaboration among mutually distrusting parties
 - ⦿ Compute on distributed data, without revealing their private information to each other

Crypto-Mania

- ⦿ Public-Key cryptography and beyond!
- ⦿ Secret computation: collaboration among mutually distrusting parties
 - ⦿ Compute on distributed data, without revealing their private information to each other
 - ⦿ Compute on encrypted data

Crypto-Mania

- ⦿ Public-Key cryptography and beyond!
- ⦿ Secret computation: collaboration among mutually distrusting parties
 - ⦿ Compute on distributed data, without revealing their private information to each other
 - ⦿ Compute on encrypted data
- ⦿ And other fancy things... with sophisticated control over more complex “access” to information

Crypto-Mania

- ⦿ Public-Key cryptography and beyond!
- ⦿ Secret computation: collaboration among mutually distrusting parties
 - ⦿ Compute on distributed data, without revealing their private information to each other
 - ⦿ Compute on encrypted data
- ⦿ And other fancy things... with sophisticated control over more complex “access” to information
- ⦿ Do it all faster, better, more conveniently and more securely (or find out if one cannot). And also make sure we know what we are trying to do.

Crypto-Mania

- Public-Key Cryptography
 - Symmetric Cryptography
 - Hash Functions
 - And so on and over again
 - Do it securely and also make sure that we are trying to do.
-
- A photograph of a group of approximately ten people, mostly men, gathered indoors. They are dressed in casual attire from the late 20th century, such as button-down shirts, blazers, and a striped sweater. Several individuals are holding white plates or cups. In the center-left, a man in a light-colored shirt is holding a large, rectangular cake decorated with a grid pattern. One man in the background has his hands raised in a peace sign. The setting appears to be a party or celebration, likely related to the theme of the slide.





Independence, Indistinguishability,
Infeasibility, Zero-Knowledge, ...



Independence, Indistinguishability,
Infeasibility, Zero-Knowledge, ...

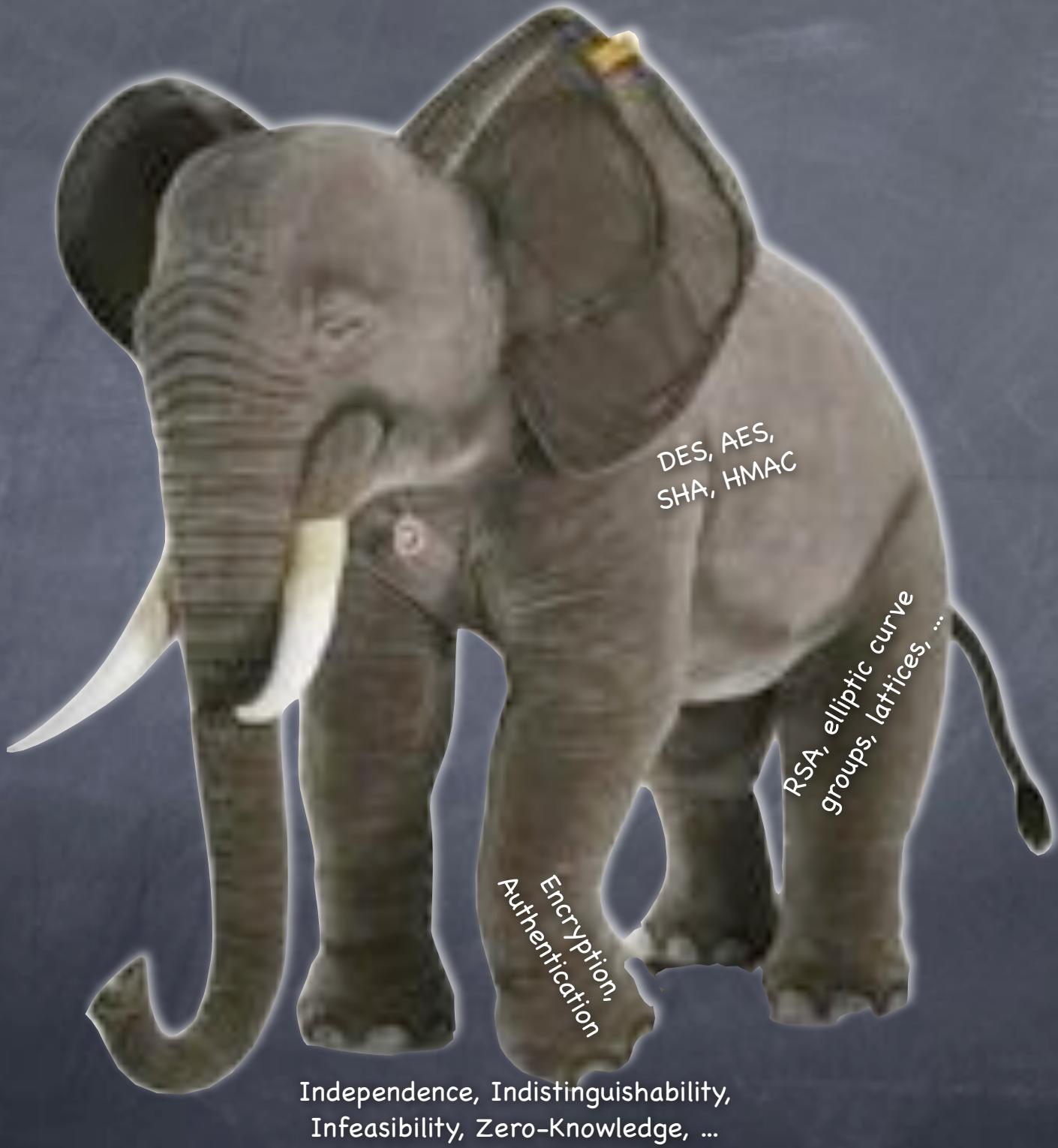
Encryption,
Authentication

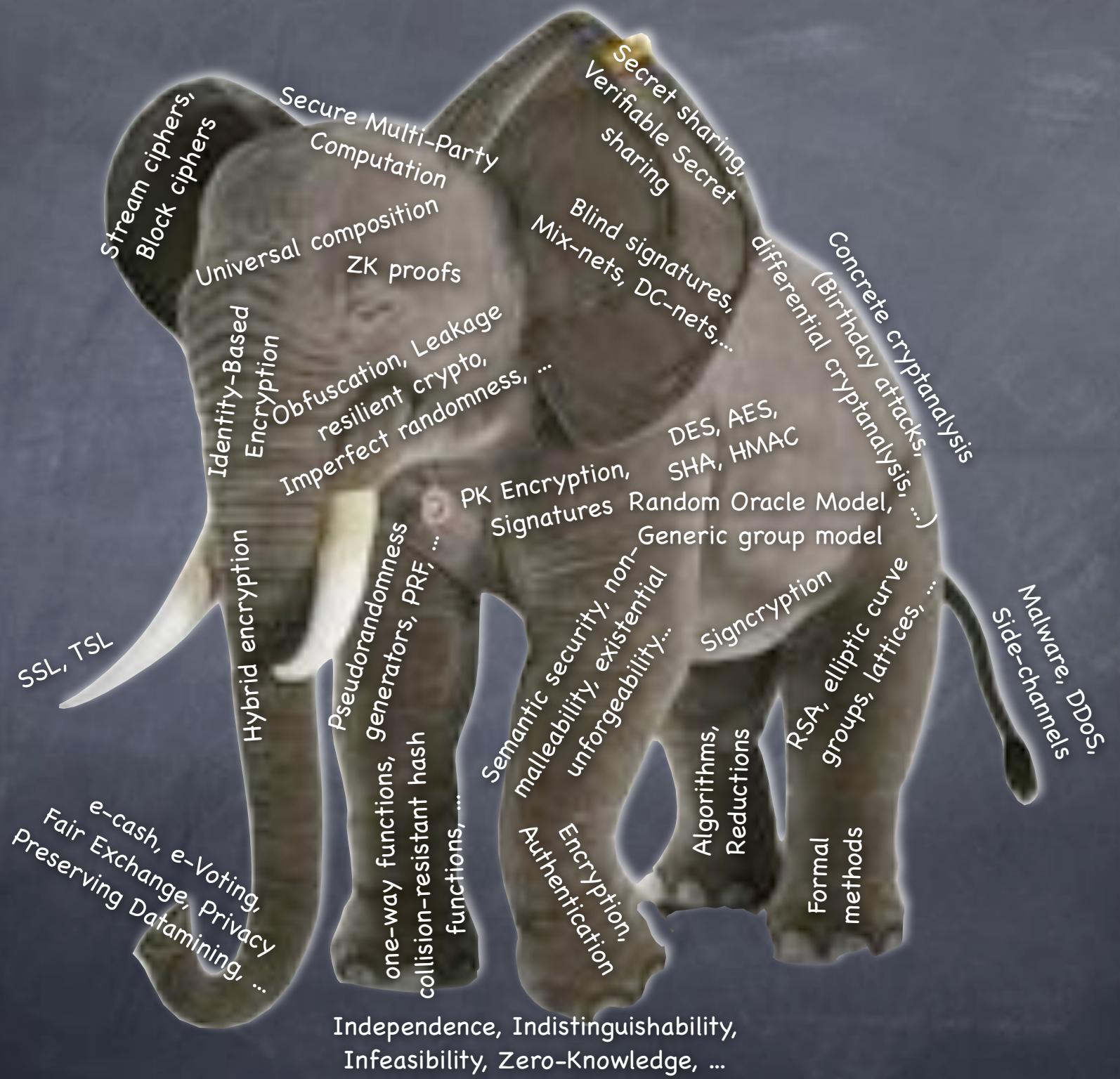


Independence, Indistinguishability,
Infeasibility, Zero-Knowledge, ...

DES, AES,
SHA, HMAC

Encryption,
Authentication





In This Course

In This Course

(how to tame the elephant...)



In This Course

(how to tame the elephant...)



- Fundamental notions of secrecy and infeasibility

In This Course

(how to tame the elephant...)



- ⦿ Fundamental notions of secrecy and infeasibility
- ⦿ Secure communication (encryption, authentication): definitions, building blocks, construction

In This Course

(how to tame the elephant...)



- ⦿ Fundamental notions of secrecy and infeasibility
- ⦿ Secure communication (encryption, authentication): definitions, building blocks, construction
- ⦿ And much more: Secure multi-party computation, computing on encrypted data, bleeding edge crypto, quick and dirty crypto...

In This Course

(how to tame the elephant...)



- ⦿ Fundamental notions of secrecy and infeasibility
- ⦿ Secure communication (encryption, authentication): definitions, building blocks, construction
- ⦿ And much more: Secure multi-party computation, computing on encrypted data, bleeding edge crypto, quick and dirty crypto...
- ⦿ Project: You can pick a topic for surveying/research, or an implementation project

In This Course

(how to tame the elephant...)



- ⦿ Fundamental notions of secrecy and infeasibility
- ⦿ Secure communication (encryption, authentication): definitions, building blocks, construction
- ⦿ And much more: Secure multi-party computation, computing on encrypted data, bleeding edge crypto, quick and dirty crypto...
- ⦿ Project: You can pick a topic for surveying/research, or an implementation project
- ⦿ A few assignments

In This Course

(how to tame the elephant...)



In This Course

(how to tame the elephant...)



- <http://www.cs.illinois.edu/class/fa10/cs598man/>

In This Course

(how to tame the elephant...)



- <http://www.cs.illinois.edu/class/fa10/cs598man/>
- Textbook for first part: Katz and Lindell

In This Course

(how to tame the elephant...)



- <http://www.cs.illinois.edu/class/fa10/cs598man/>
- Textbook for first part: Katz and Lindell
- There's a blog and a wiki.

In This Course

(how to tame the elephant...)



- ☞ <http://www.cs.illinois.edu/class/fa10/cs598man/>
- ☞ Textbook for first part: Katz and Lindell
- ☞ There's a blog and a wiki.
- ☞ Office Hours:

In This Course

(how to tame the elephant...)



- ☞ <http://www.cs.illinois.edu/class/fa10/cs598man/>
- ☞ Textbook for first part: Katz and Lindell
- ☞ There's a blog and a wiki.
- ☞ Office Hours:
 - ☞ Thursday 2:00-3:00 PM (tentative)