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?

Or rather the lack of it?

Uncertainty

The word is **Entropy**

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
What is information?

Or rather the lack of it?

Uncertainty

The word is **Entropy**

Borrowed from thermodynamics

An inherently “probabilistic” notion
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)
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
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.
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
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
Steve 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
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
- 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!
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!

James Ellis
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
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

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

Encryption, Authentication

DES, AES, SHA, HMAC
Independence, Indistinguishability, Infeasibility, Zero-Knowledge, ...

RSA, elliptic curve groups, lattices, ...

DES, AES, SHA, HMAC

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

One-way functions, Collision-resistant hash functions, ...

Semantic security, Non-malleability, Existential unforgeability...

Obfuscation, Leakage resilient crypto, Imperfect randomness, ...

PK Encryption, Signatures Random Oracle Model, Generic group model

Identity-Based Encryption

Universal composition

Secure Multi-Party Computation

ZK proofs

Blind signatures, Mix-nets, DC-nets...

differential cryptanalysis, ...

Concrete cryptography

DES, AES, SHA, HMAC

Identity-Based Encryption

Secure Multi-Party Computation

ZK proofs

Blind signatures, Mix-nets, DC-nets...

Concrete cryptography

DES, AES, SHA, HMAC
In This Course
In This Course
(how to tame the elephant...)
In This Course

(how to tame the elephant...)

Fundamental notions: secrecy, infeasibility
In This Course
(how to tame the elephant...)

- Fundamental notions: **secrecy, infeasibility**
- Secure communication (encryption, authentication): definitions, building blocks, construction
In This Course
(how to tame the elephant...)

Fundamental notions: **secrecy, 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: secrecy, 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: secrecy, 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...)

![Elephant]
In This Course
(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2013/
In This Course
(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2013/

Textbook for first part: Katz and Lindell
In This Course

(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2013/

Textbook for first part: Katz and Lindell

Cryptutor Wiki
In This Course
(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2013/

Textbook for first part: Katz and Lindell

Cryptutor Wiki

Office Hours: TBA