Cryptography

Lecture 0

Manoj Prabhakaran

University of Illinois Urbana-Champaign
“Properly implemented strong crypto systems are one of the few things that you can rely on.”
“Properly implemented strong crypto systems are one of the few things that you can rely on.”

“... Unfortunately, endpoint security is so terrifically weak that [the adversary] can frequently find ways around it.”
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.

A tool for enforcing policies on who can learn and/or influence information.
What is Cryptography?

It's all about controlling access to information.

A tool for enforcing policies on who can learn and/or influence 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

Rudolf Clausius
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

An inherently “probabilistic” notion

Rudolf Clausius

Ludwig Boltzmann

Claude Shannon
What is information?

Claude Shannon
What is information?

Information Theory: ways to quantify information
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
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”
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

Impossible in the information-theoretic sense: a truly random string cannot be compressed
Compressed Secret-Keys

Impossible in the information-theoretic sense: a truly random string cannot be compressed

But possible against computationally bounded players: use pseudo-random strings!
Compressed Secret-Keys

Impossible in the information-theoretic sense: a truly random string cannot be compressed.

But possible against computationally bounded players: use pseudo-random strings!

Pseudo-random number generator
Compressed Secret-Keys

Impossible in the information-theoretic sense:
  a truly random string cannot be compressed

But possible against computationally bounded players:
  use pseudo-random strings!

Pseudo-random number generator

a.k.a Stream Cipher
Compressed Secret-Keys

Impossible in the information-theoretic sense: a truly random string cannot be compressed

But possible against computationally bounded players: use pseudo-random strings!

Pseudo-random number generator

a.k.a Stream Cipher

Generate a long string of random-looking bits from a short random seed
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

“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

Malcolm Williamson

Clifford Cocks

Merkle, Hellman, Diffie
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.
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
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
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...)
In This Course
(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2016/
In This Course
(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2016/

A textbook for the first part of the course:
Katz and Lindell
In This Course
(how to tame the elephant...)

http://courses.engr.illinois.edu/cs598man/sp2016/

A textbook for the first part of the course: Katz and Lindell

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

http://courses.engr.illinois.edu/cs598man/sp2016/

A textbook for the first part of the course:
Katz and Lindell

Cryptutor Wiki

Office Hours: TBA
The Big Picture

Cryptography
The Big Picture

Cryptography

Information Security
The Big Picture

Cryptography

Information Security

Complexity Theory
The Big Picture

- Cryptography
- Information Theory
- Complexity Theory
- Information Security
The Big Picture

- Cryptography
- Information Theory
- Information Security
- Number Theory, Algebra
- Complexity Theory
The Big Picture

- Information Theory
- Cryptography
- Formal Methods
- Information Security
- Complexity Theory
- Number Theory, Algebra
- Combinatorics, Graph theory
- Number Theory, Algebra
- Combinatorics, Graph theory
Cryptography is only a small (but vital) part of information security.
Cryptography is only a small (but vital) part of information security.

Cryptography studies several problems which may not be of immediate use in information security, but is important in building its own foundations/in establishing links with other areas.

The Big Picture
Cryptography is only a small (but vital) part of information security.

Cryptography studies several problems which may not be of immediate use in information security, but is important in building its own foundations/in establishing links with other areas.

Cryptography has an “engineering” component (e.g. SSL/TSL) and a “science” component (e.g. definitions, proofs).
Puzzle #1
Puzzle #1

Alice and Bob hold secret numbers $x$ and $y$ in $\{0,..,n\}$ resp.
Puzzle #1

Alice and Bob hold secret numbers $x$ and $y$ in $\{0, \ldots, n\}$ resp.

Carol wants to learn $x+y$. Alice and Bob are OK with that.
Puzzle #1

Alice and Bob hold secret numbers \(x\) and \(y\) in \(\{0, \ldots, n\}\) resp.

Carol wants to learn \(x+y\). Alice and Bob are OK with that.

But they don’t want Carol/each other to learn anything else!
Puzzle #1

Alice and Bob hold secret numbers $x$ and $y$ in $\{0, \ldots, n\}$ resp.
Carol wants to learn $x+y$. Alice and Bob are OK with that.
But they don’t want Carol/each other to learn anything else!

i.e., Alice should learn nothing about $y$, nor Bob about $x$. Carol shouldn’t learn anything else about $x,y$ “other than” $x+y$
Puzzle #1

Alice and Bob hold secret numbers $x$ and $y$ in $\{0,..,n\}$ resp.

Carol wants to learn $x+y$. Alice and Bob are OK with that.

But they don’t want Carol/each other to learn anything else!

i.e., Alice should learn nothing about $y$, nor Bob about $x$. Carol shouldn’t learn anything else about $x,y$ “other than” $x+y$

Can they do it, just by talking to each other (using private channels between every pair of parties)?
Puzzle #2

Alice and Bob hold secret bits $x$ and $y$

Carol wants to learn $x \land y$. Alice and Bob are OK with that.

But they don't want Carol/each other to learn anything else!

i.e., Alice should learn nothing about $y$, nor Bob about $x$. Carol shouldn't learn anything else about $x,y$ “other than” $x \land y$

Can they do it, just by talking to each other (using private channels between every pair of parties)?