Less theoretical,
with a hands-on component

Renewed

Cryptography

and Network Security - I

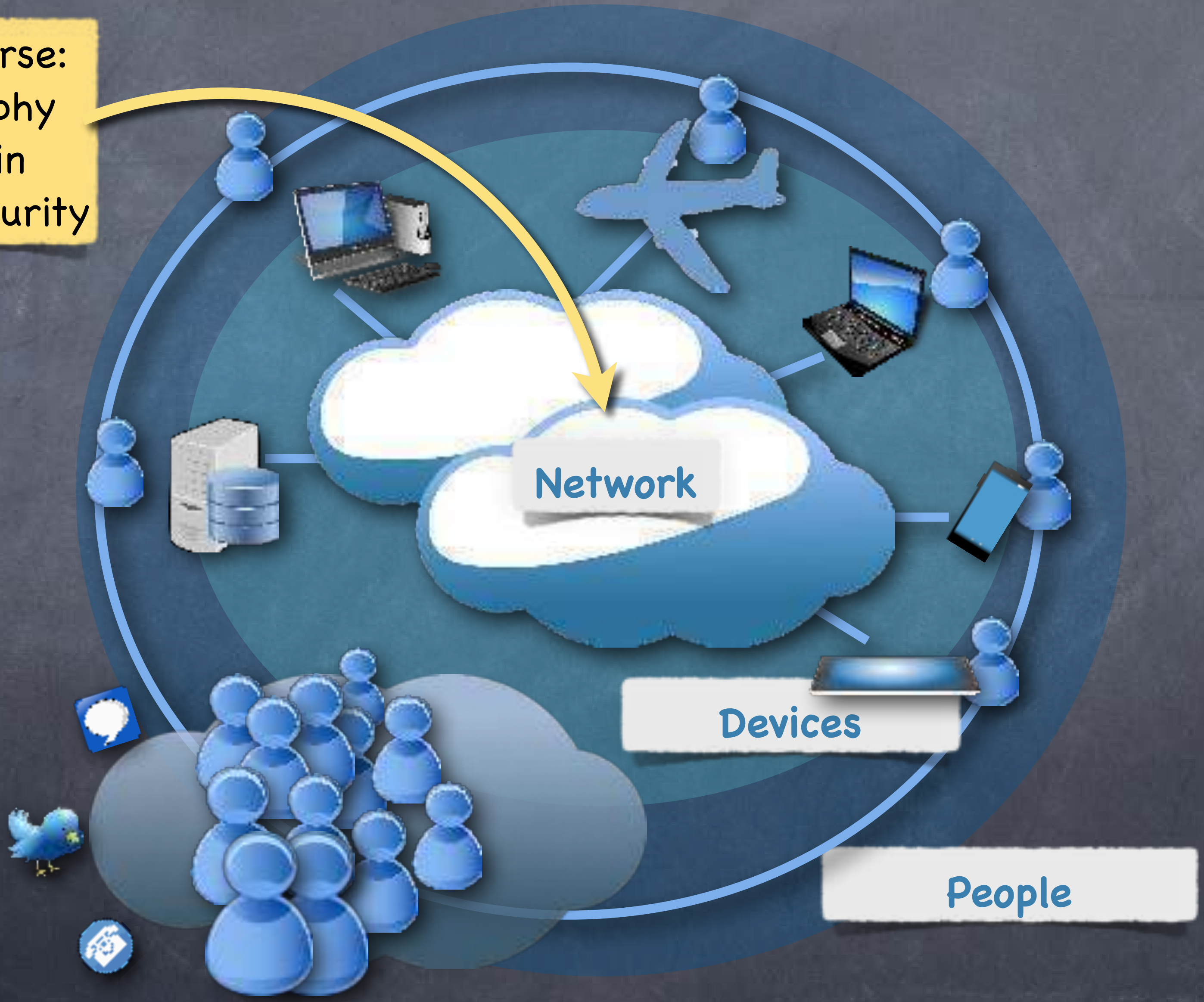
Lecture 0

Manoj Prabhakaran

IIT Bombay

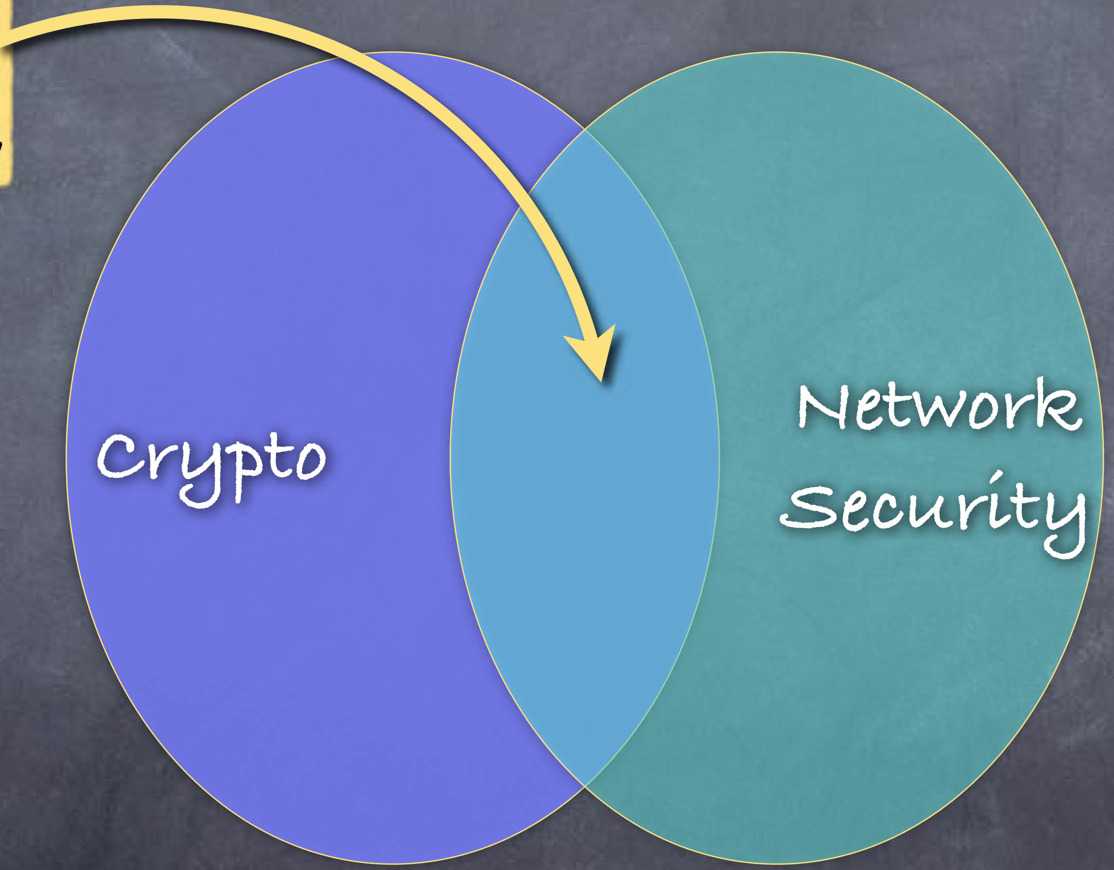
Security

In this course: Cryptography as used in network security



Cryptography & Security

In this course: Cryptography as used in network security



In the News

- "Properly implemented strong crypto systems are one of the few things that you can rely on."

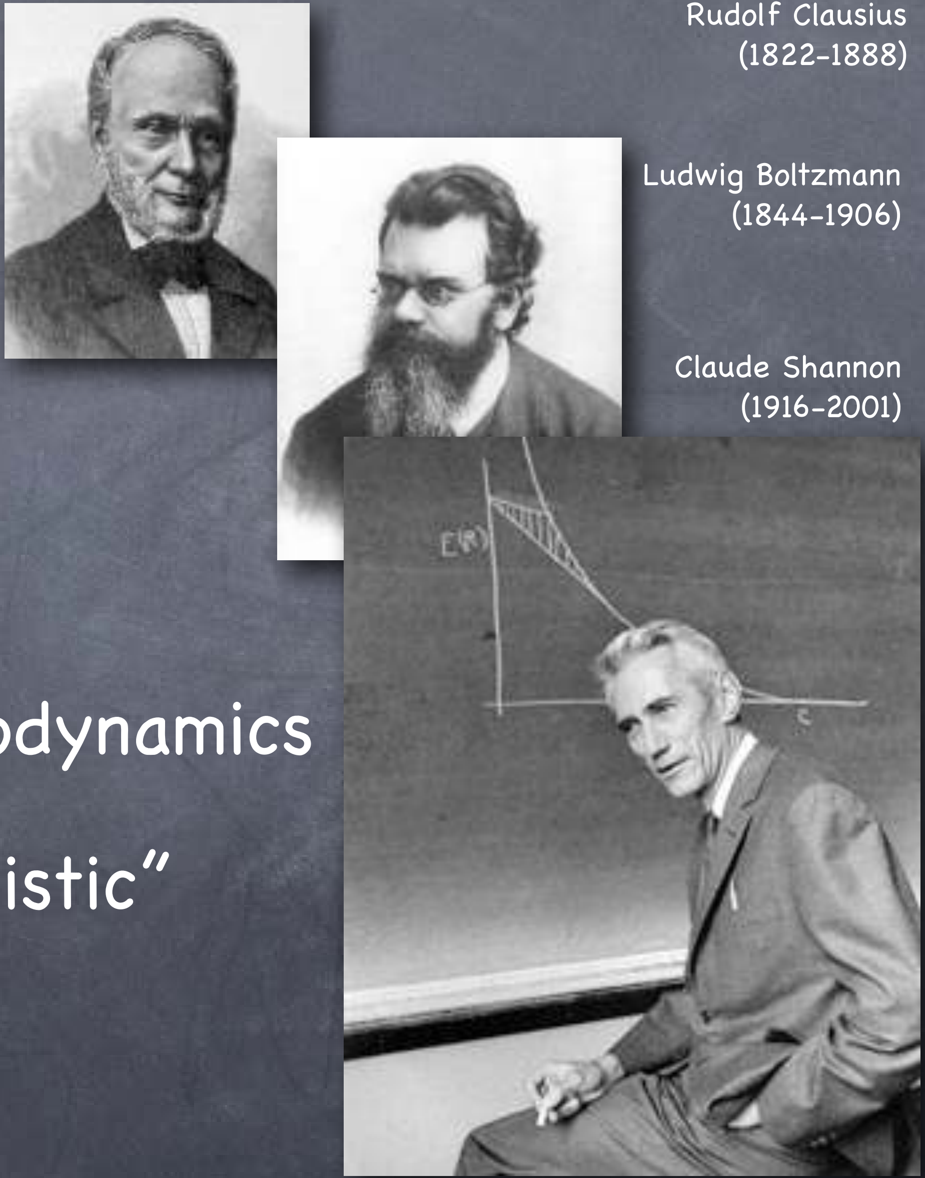
- "... Unfortunately, endpoint security is so terrifically weak that [the adversary] can frequently find ways around it."

What is Cryptography?

- 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?

- Or rather the lack of it?
  - Uncertainty
  - Measured using Entropy
    - Borrowed from thermodynamics
    - An inherently “probabilistic” notion



Rudolf Clausius
(1822-1888)

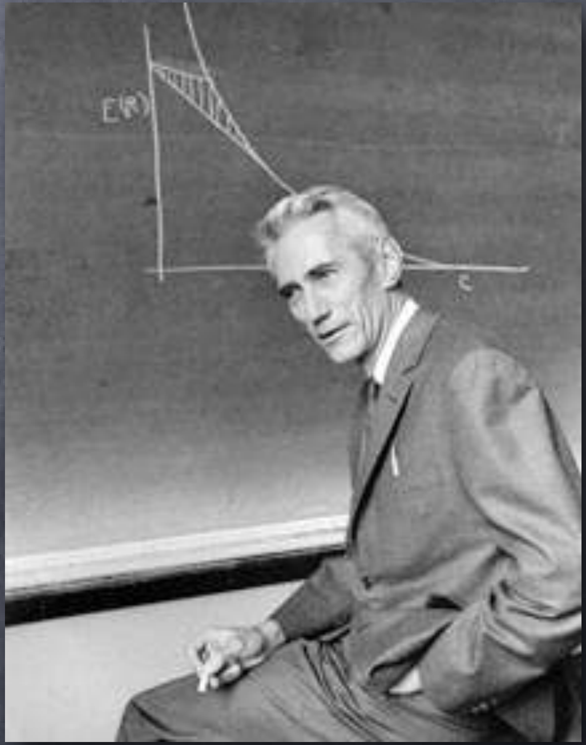
Ludwig Boltzmann
(1844-1906)

Claude Shannon
(1916-2001)

What is information?

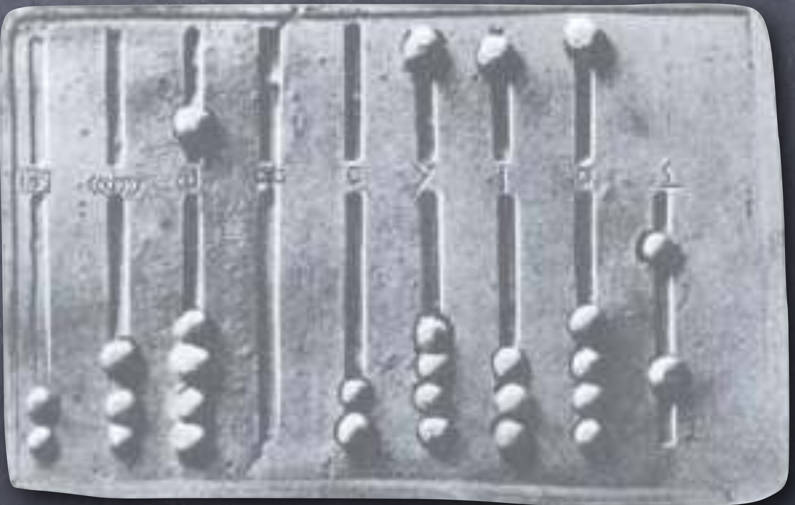
- Information Theory: ways to quantify information
  - Application 1: to study efficiency of communication (compression, error-correction)
  - Application 2: to study the possibility of secret communication
    - The latter turned out to be a relatively easy question! Secret communication possible only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

Claude Shannon
(1916-2001)



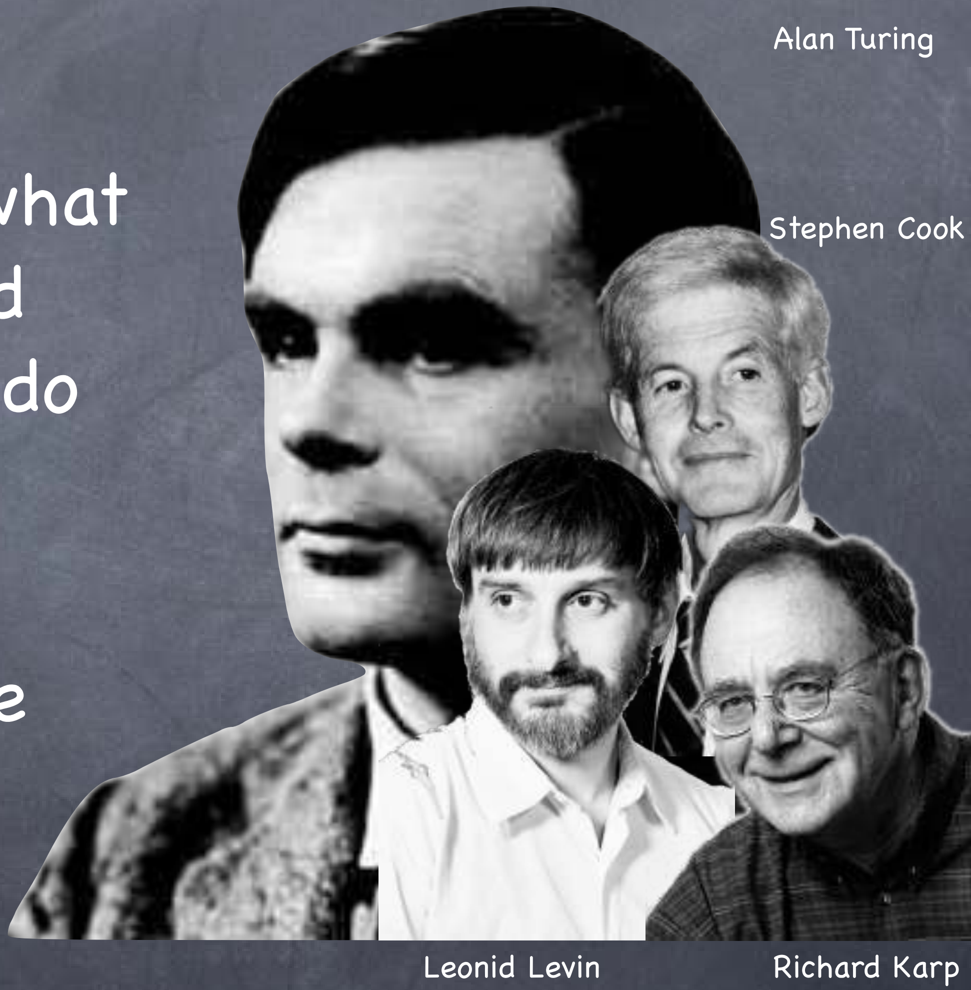
Access to Information

- 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

- 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

- 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

Manuel Blum

Andy Yao

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

Malcolm Williamson

Clifford Cocks

James Ellis

Merkle, Hellman, Diffie

Shamir, Rivest, Adleman

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.

Turing Awards

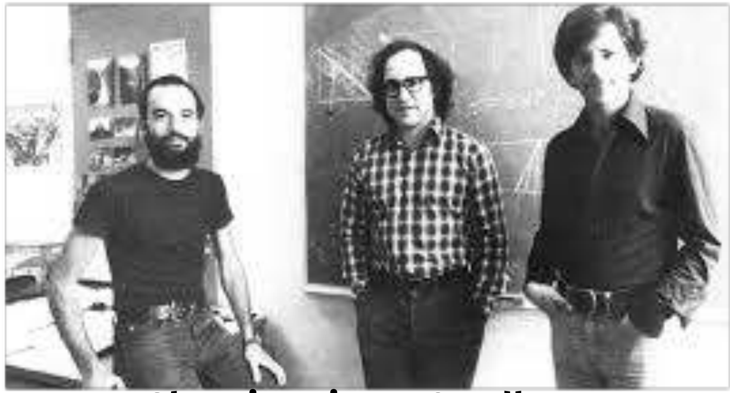
- For theoretical cryptographers:

(Merkle) Hellman & Diffie
Turing Award '15

Goldwasser & Micali
Turing Award '12

Manuel Blum
Turing Award '95

Andrew Yao
Turing Award '00



Shamir , Rivest & Adleman
Turing Award '02

In This Course
Cryptography

- Secure communication

	Shared-Key	Public-Key
Encryption	SKE	PKE
Authentication	MAC	Signature

- Zero-Knowledge Proofs: a basic introduction
- Mathematical background: Some Probability, a little bit of Groups and Number Theory, Definitions and a little bit of proofs
- Hands-on content: playing around with software tools

In This Course
Network Security

- A peek into TLS, IPSec, ...
- Issues not discussed in this course:
  - Complexity due to support for extra efficiency/backward compatibility/new features
  - Buggy implementations (software & hardware)
  - Gap between abstract and real-life models: side-channels
  - Endpoint security
  - Often informal/ill-specified security goals
  - Human factors, trust, identity, current and legacy technology, ...

Course Logistics

- Please attend all the lectures
  - Some of the lecture sessions will be for hands-on labs
- Grading:
  - Mid/End-semester Exams (60%)
  - ≈3 HW assignments (15%)
  - Course project (15%)
  - Labs (10%)
- See Moodle for announcements