Cryptography
and Network Security

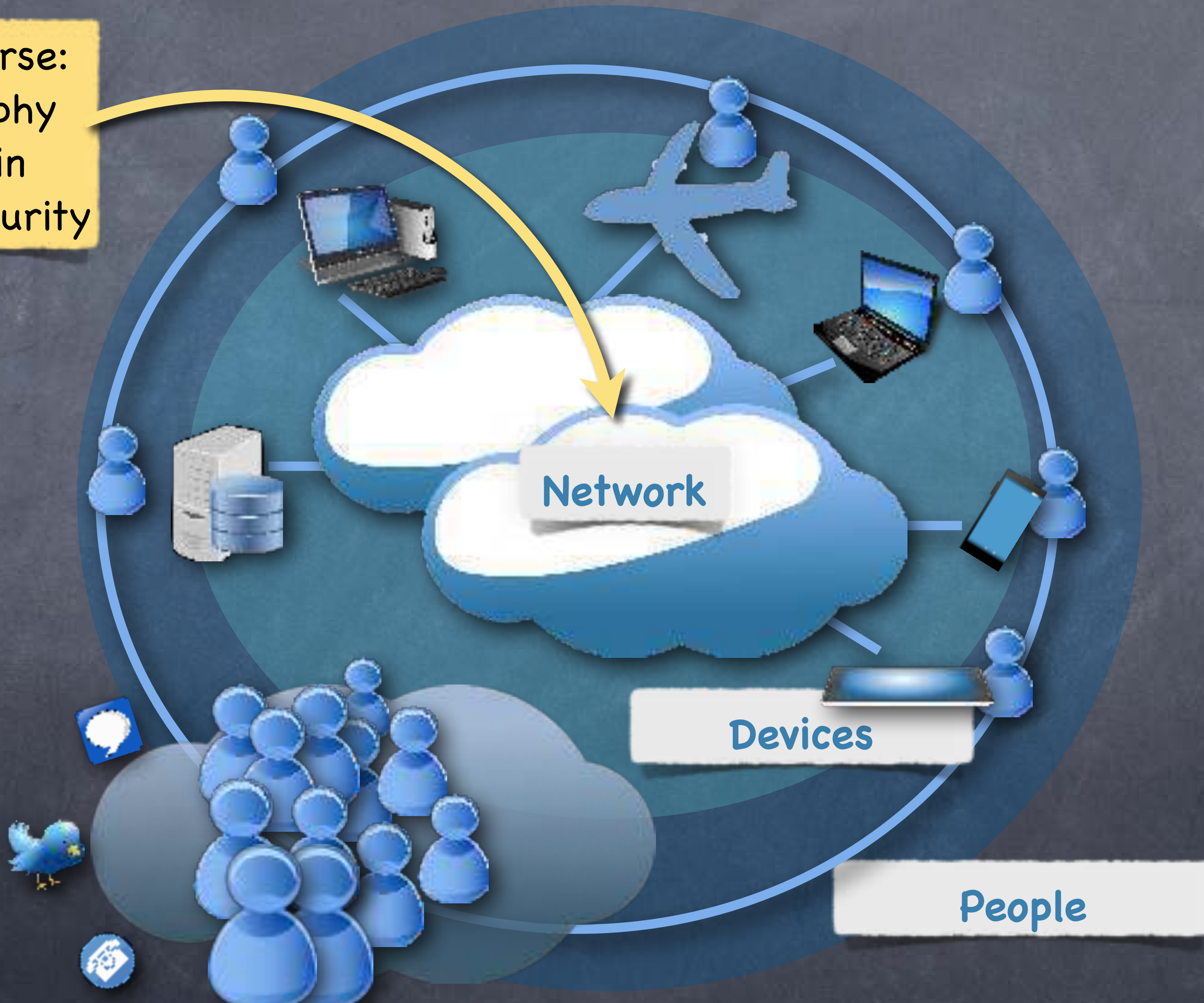
Lecture 0

Manoj Prabhakaran

IIT Bombay

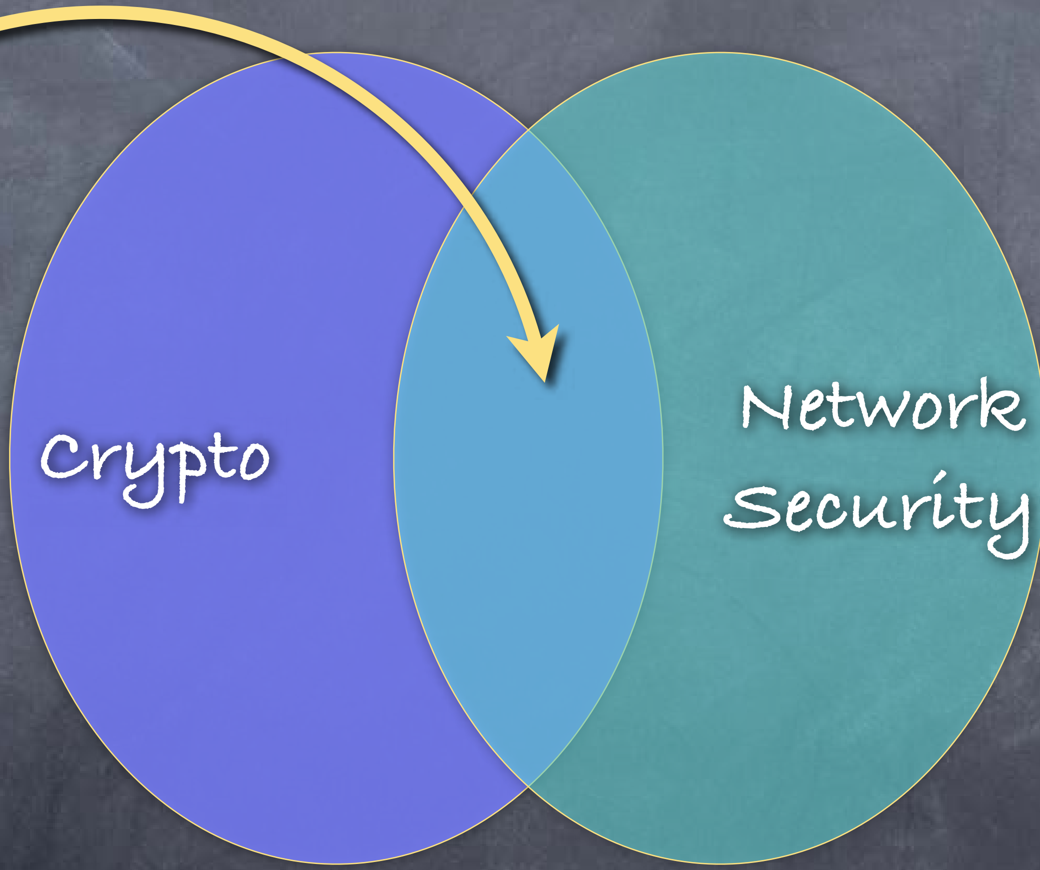
Security

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?

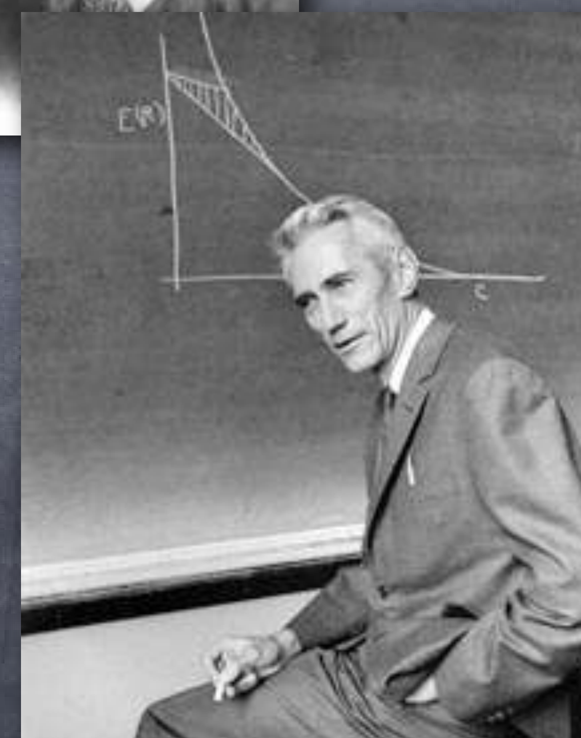
- It's all about controlling access to information
  - A tool for enforcing policies on who can learn and/or influence information
  - Do we know what we are talking about?

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)

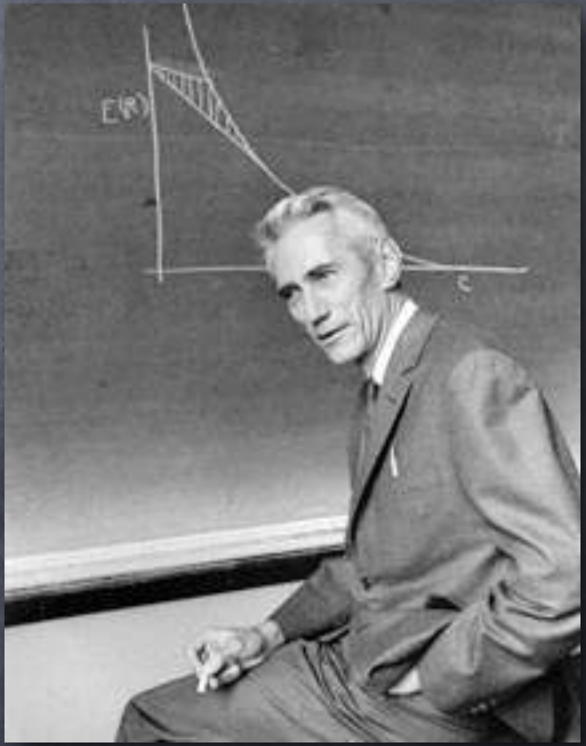


Claude Shannon (1916-2001)

What is information?

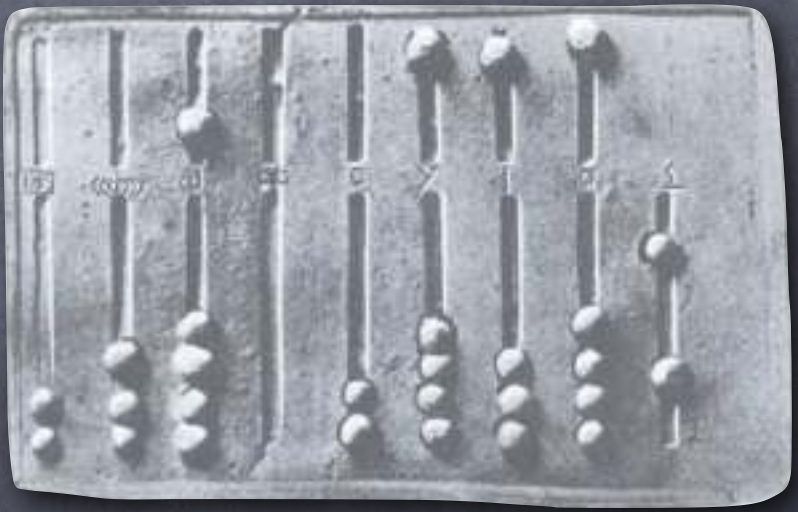
- Information Theory: ways to quantify information
  - Application 1: to study efficiency of communication (compression, error-correction)
  - Application 2: to study the possibility of secret communication
    - The latter turned out to be a relatively easy question! Secret communication possible only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

Claude Shannon
(1916-2001)



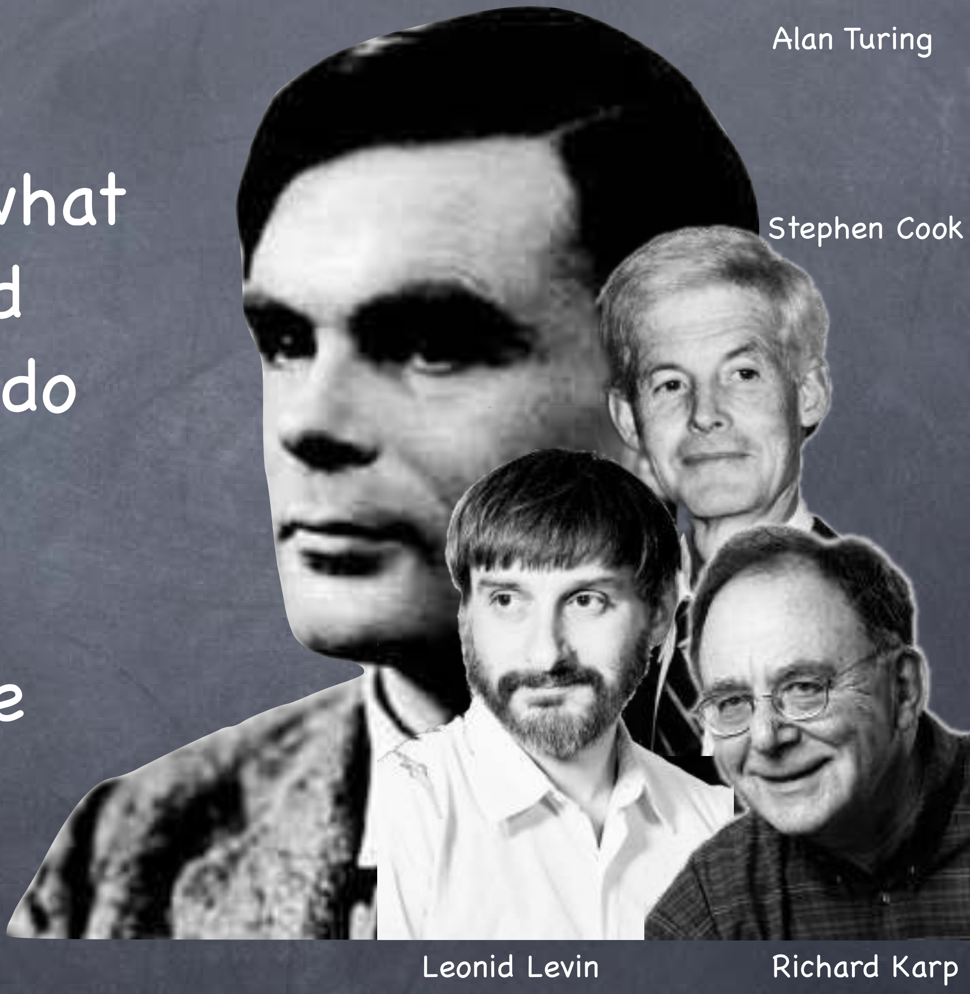
Access to Information

- 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

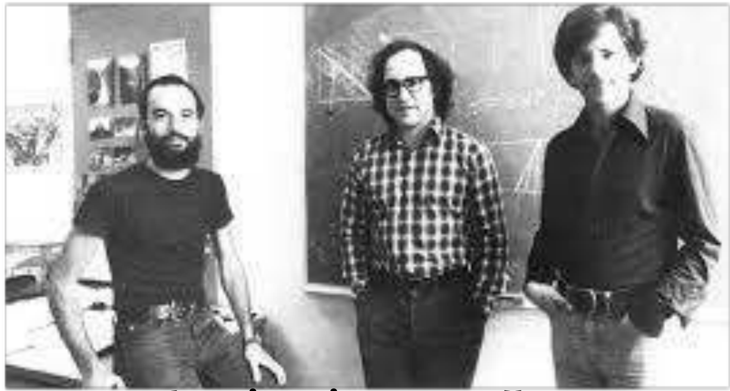
- For theoretical cryptographers:

(Merkle) Hellman & Diffie
Turing Award ‘15

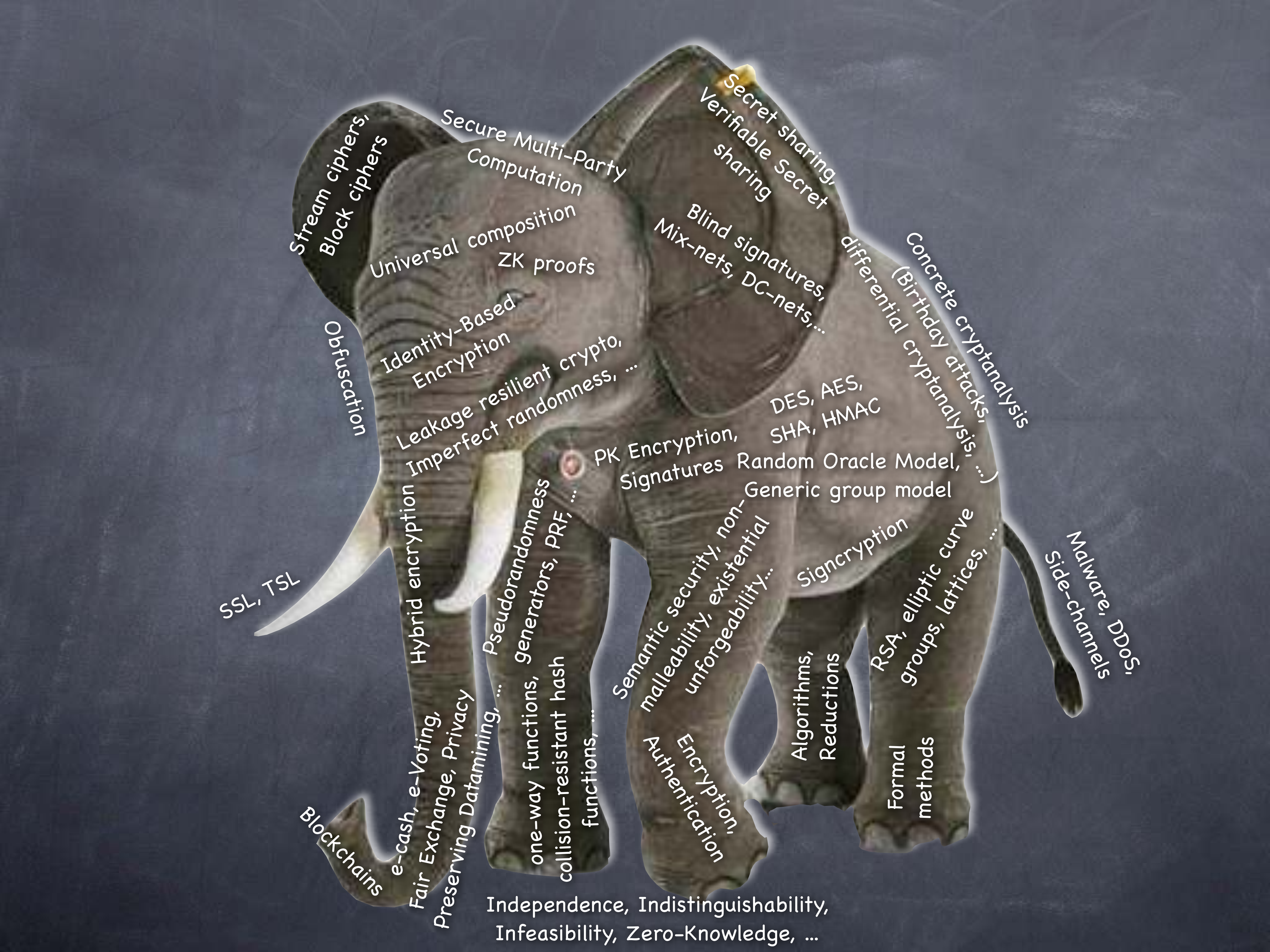
Goldwasser & Micali
Turing Award ‘12

Manuel Blum
Turing Award ‘95

Andrew Yao
Turing Award ‘00



Shamir , Rivest & Adleman
Turing Award ‘02


Stream ciphers,
Block ciphers
Secure Multi-Party
Computation
Secret sharing,
Verifiable Secret
sharing
Universal composition
ZK proofs
Blind signatures,
Mix-nets, DC-nets,...
Concrete cryptanalysis
(Birthday attacks,
differential cryptanalysis, ...)
Obfuscation
Identity-Based
Encryption
Leakage resilient crypto,
Imperfect randomness, ...
DES, AES,
SHA, HMAC
PK Encryption,
Signatures
Random Oracle Model,
Generic group model
Hybrid encryption
Pseudorandomness
generators, PRF, ...
one-way functions,
collision-resistant hash
functions, ...
Semantic security, non-
malleability, existential
unforgeability...
Signcryption
RSA, elliptic curve
groups, lattices, ...
Malware, DDoS,
Side-channels
SSL, TSL
e-cash, e-Voting,
Fair Exchange, Privacy
Preserving Datamining, ...
Blockchains
Encryption,
Authentication
Algorithms,
Reductions
Formal
methods
Independence, Indistinguishability,
Infeasibility, Zero-Knowledge, ...

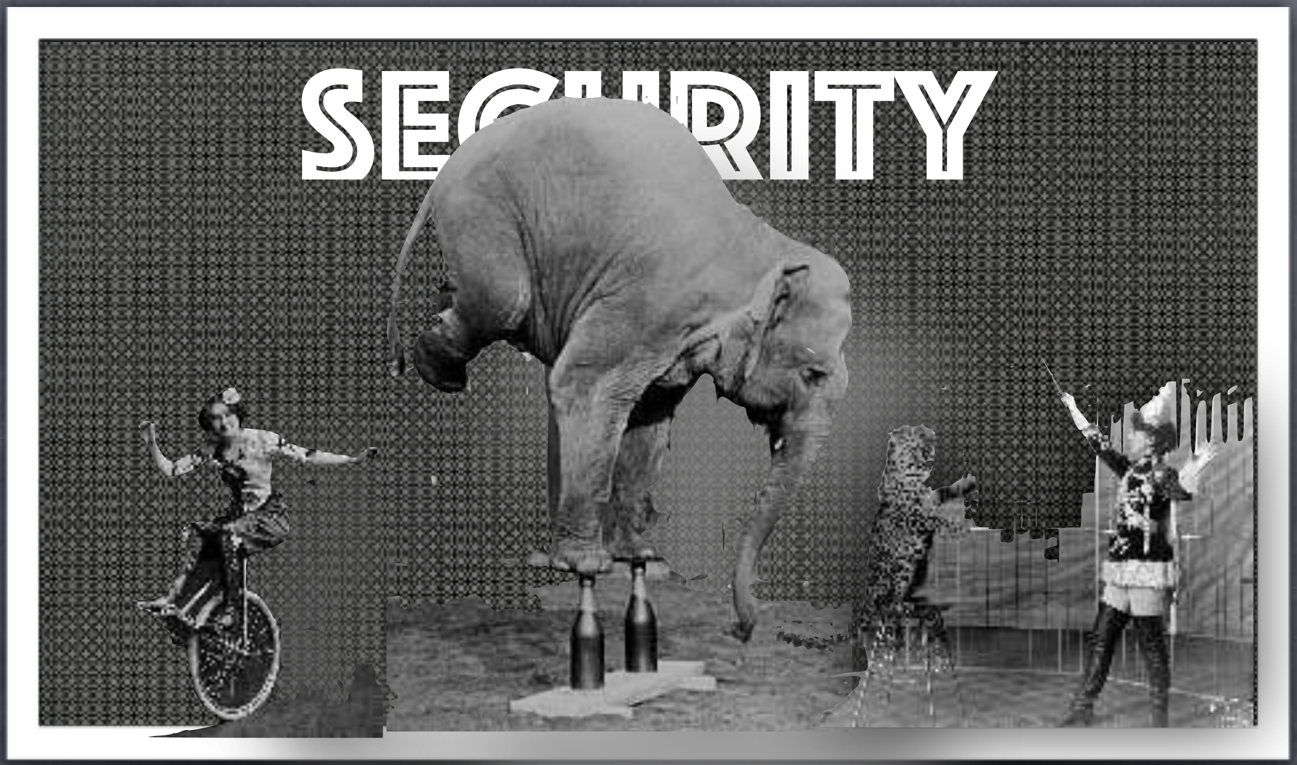
In This Course
(Petting the Elephant)

- Fundamental notions: **secrecy**, **infeasibility**
- Secure communication

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

- Mathematical content:
  - Some Probability
  - A little bit of Groups and Number Theory
  - Definitions and proofs

Also a Glimpse of...

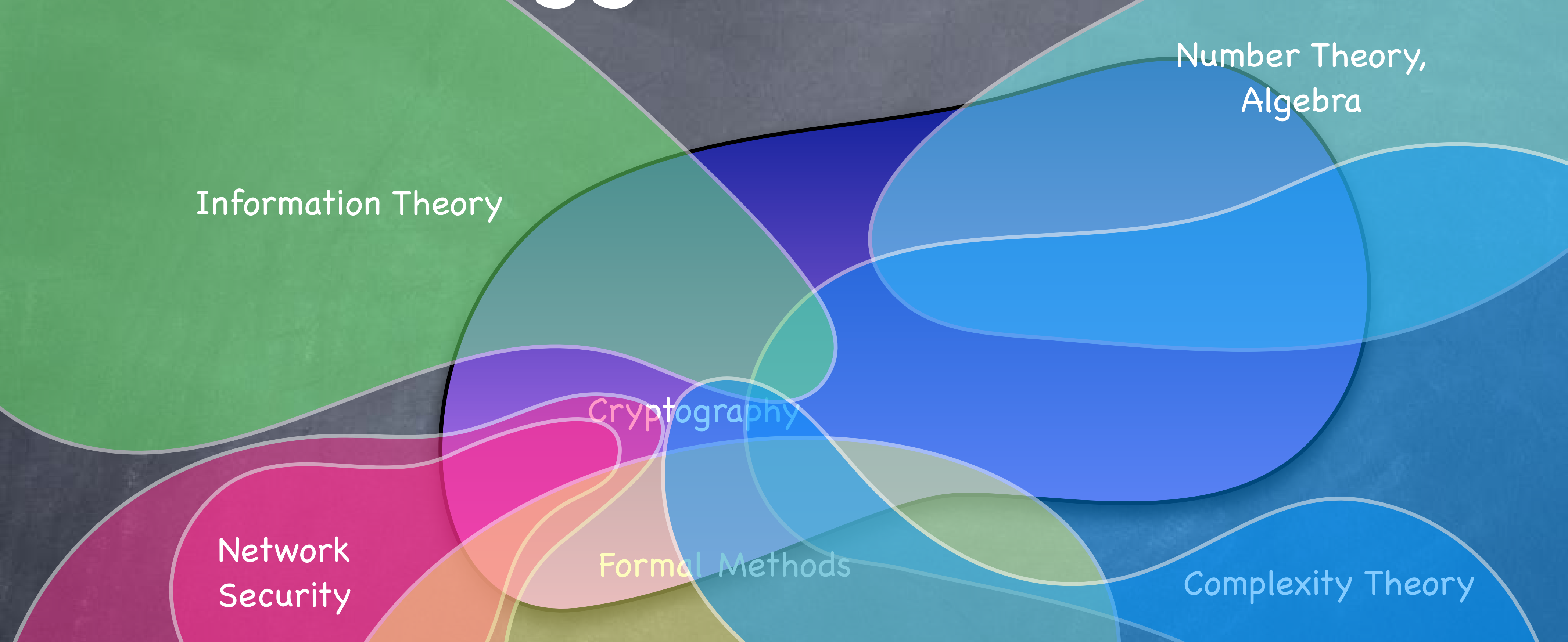


- Security involves many (f)actors other than crypto
- Crypto is a tool that when correctly used can help us greatly enhance (and understand) security

Network Security

- How to use cryptography to achieve security goals in a real-life scenario?
- Several new issues:
  - More complex (often informal/ill-specified) security goals
  - Complexity due to support for extra efficiency/backward compatibility/new features
  - Buggy implementations (software & hardware)
  - Gap between abstract and real-life models: side-channels
  - Human factors, trust, identity, current and legacy technology, ...

Bigger Picture



Cryptography is just one of the tools used in 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

Many powerful cryptographic tools remain un(der)utilised in practice!

Course Logistics

- Lectures
  - Recordings to be posted on Moodle
- Grading:
  - Mid/End-semester Exams (65%)
    - One during the mid-semester exam week
  - ≈3 HW assignments (15%)
  - Course project (20%)
- "Theory" course: no significant programming requirement, but course project could be a programming project

Course Logistics

- Live and/or recorded lectures
  - See Moodle
- Online forum: piazza.com/iitb.ac.in/spring2021/cs406
- Course webpage: see cse.iitb.ac.in/~mp/teach/

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 $x \wedge y$. 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" $x \wedge y$
- Can they do it, just by talking to each other (using private channels between every pair of parties)?