CPSC 530/630: INFORMATION THEORY & SECURITY

- Rei Safavi-Naini, ICT 636, rei@ucalgary.ca

- Classes: TR 15:30-16:45, Rm ENG 230
- Consultation: TR 13:00-14:00, or by appointment

- Teaching Assistants:
- Ali Poostindouz alireza.poostindouz@ucalgary.ca
- Mahmudun Nabi mahmudun.nabi1@ucalgary.ca
- Shuai Li shuai.li1@ucalgary.ca
-
- TUT 1: TR 17:00 - 17:50 MS 217
- TUT 2: TR 11:00 - 11:50 ST 063

- No Registrar's scheduled final examination.

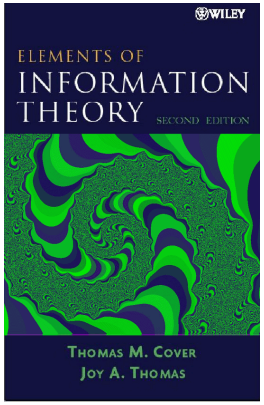
CPSC 530

Component(s)	Weighting %
Assignment	40%
Midterm	20%
Project	40%

CPSC 630

Component(s)	Weighting %
Assignment	30%
Midterm	20%
Project	50%

Resources



Reference books:

- Elements of Information Theory: **(CT)**
  Thomas M. Cover, Joy A. Thomas -2006

http://www.eecs.harvard.edu/cs286r/courses/fall10/papers/Chapter2.pdf

- Introduction to Modern Cryptography (2nd edition) **(KL)**
  Jonathan Katz and Yehuda Lindell
  Online

- Slides, assignments and reading material: D2L

Working in groups

- Form groups of 4-5 students for the whole semester
  - Due by Friday Sept 21
  - Send me & Shuai Li, an email with names, and student IDs of group members.
  - Those without a group will be put in groups.

- Assignment: Individual submission
  - Group discussion is encouraged.
- Project: Group submission

  All submissions should be typeset.

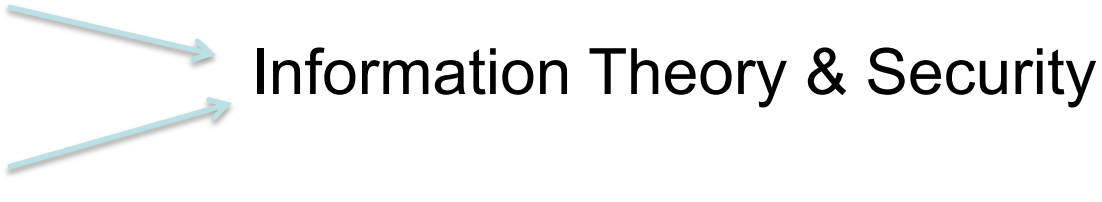
- Questions about course/assignments:
  - Tutorial hour
  - Bulletin board and email

	Tue	**Thur**	
Week 1		Sept 6	
Week 2	Sept 11	Sept 13 Project Outline	
Week 3	Sep 18	Sep 20	Sept 21 Groups Formed
Week 4	Sept 25	Sept 27	
Week 5	Oct 2	Oct 4	
Week 6	Oct 9	Oct 11	
Week 7	Oct 16	Oct 18	
Week 8	Oct 23	Oct 25	
Week 9	Oct 30 MID TERM	Nov 1	
Week 10	Nov 6	Nov 8	
Semester break	Nov 13	Nov 15	
Week 11	Nov 20	Nov22	
Week 12	Nov 27	Nov 29	
Week 13	Dec 4	Dec 6	

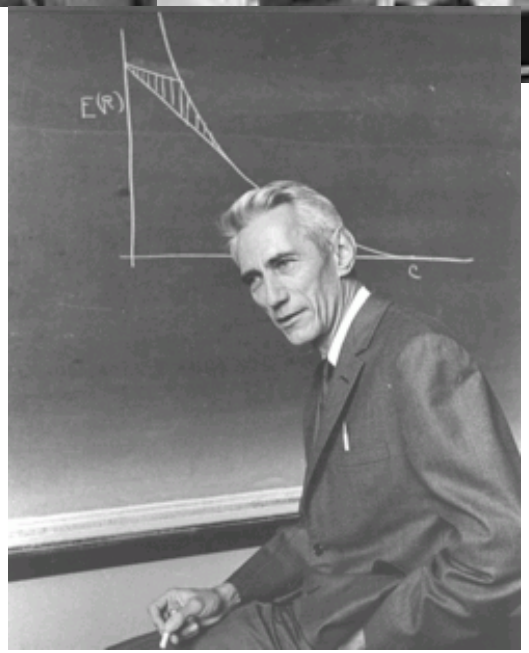
Tentative course schedule

Information Theory & Security

1. Information Theory
2. Information Security



Quiz: Who is this person?



- Claude E. Shannon
- 1916-2001

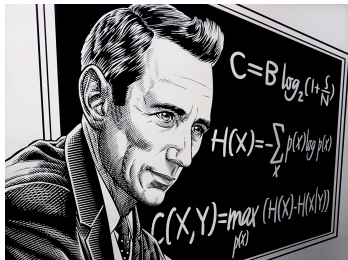
C.E. Shannon:

The Father of The Information Age

- www.youtube.com/watch?v=z2Whj_nL-x8
- www.youtube.com/watch?v=vPKkXibQXGA

- www.newyorker.com/tech/elements/claude-shannon-the-father-of-the-information-age-turns-1100100
- spectrum.ieee.org/tech-talk/telecom/internet/bell-labs-looks-at-claude-shannon-legacy-future-of-information-age

- The Bit Player (2018)



Contributions

- Information theory
- Digital communication – error correction
- Compression - Mpeg, Jpeg, MP3, Zip…

- Boolean algebra for digital circuits
- Digital computers
- Learning and artificial intelligence

http://www.itsoc.org/resources/Shannon-Centenary

Shannon's Work and Its Legacy, M. Effros and H. V. Poor.

Information Theory

1916-2001

- A mathematical definition of information measure and application to communication (1948):

  'A Mathematical Theory of Communication'

  – http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

- Shannon proposed the first formal treatment of cryptography (secrecy) (1949).

  'Communication Theory of Secrecy Systems'

  – http://www.mast.queensu.ca/~math474/shannon-secrecy49.pdf

What type of information?

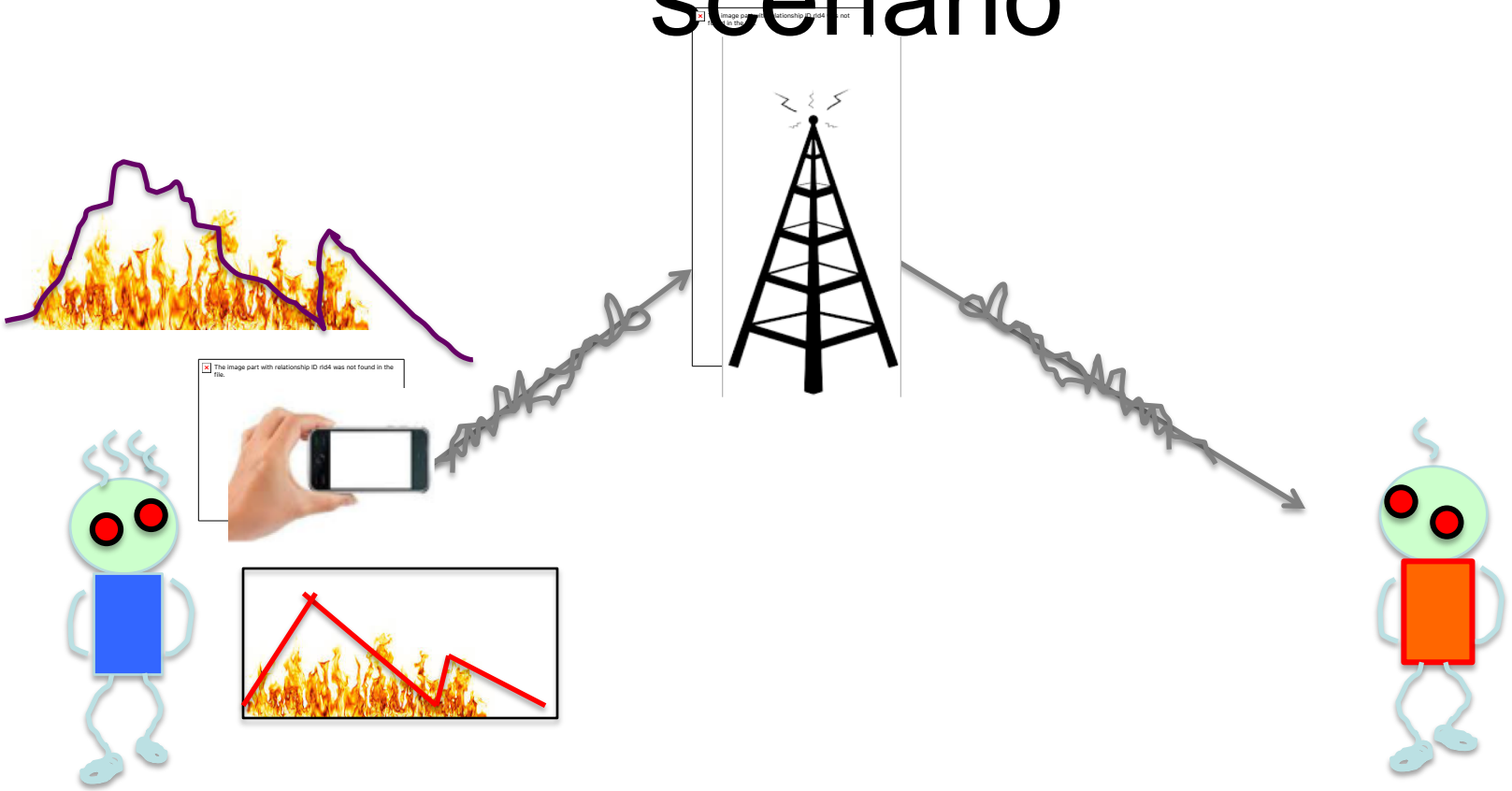
- "Information": an overloaded term
  - Information sheet of a course
  - Information Sciences:

    "an interdisciplinary field primarily concerned with the analysis, collection, classification, manipulation, storage, retrieval, movement, dissemination, and protection of information"

  - "Let me give you some information"

  - Non-tangible – illusive concept

Information communication scenario



- How much “information” to send? (Technical)
  - How fast?
- The meaning of the picture (Semantic)
- Bob’s action (Effectiveness)

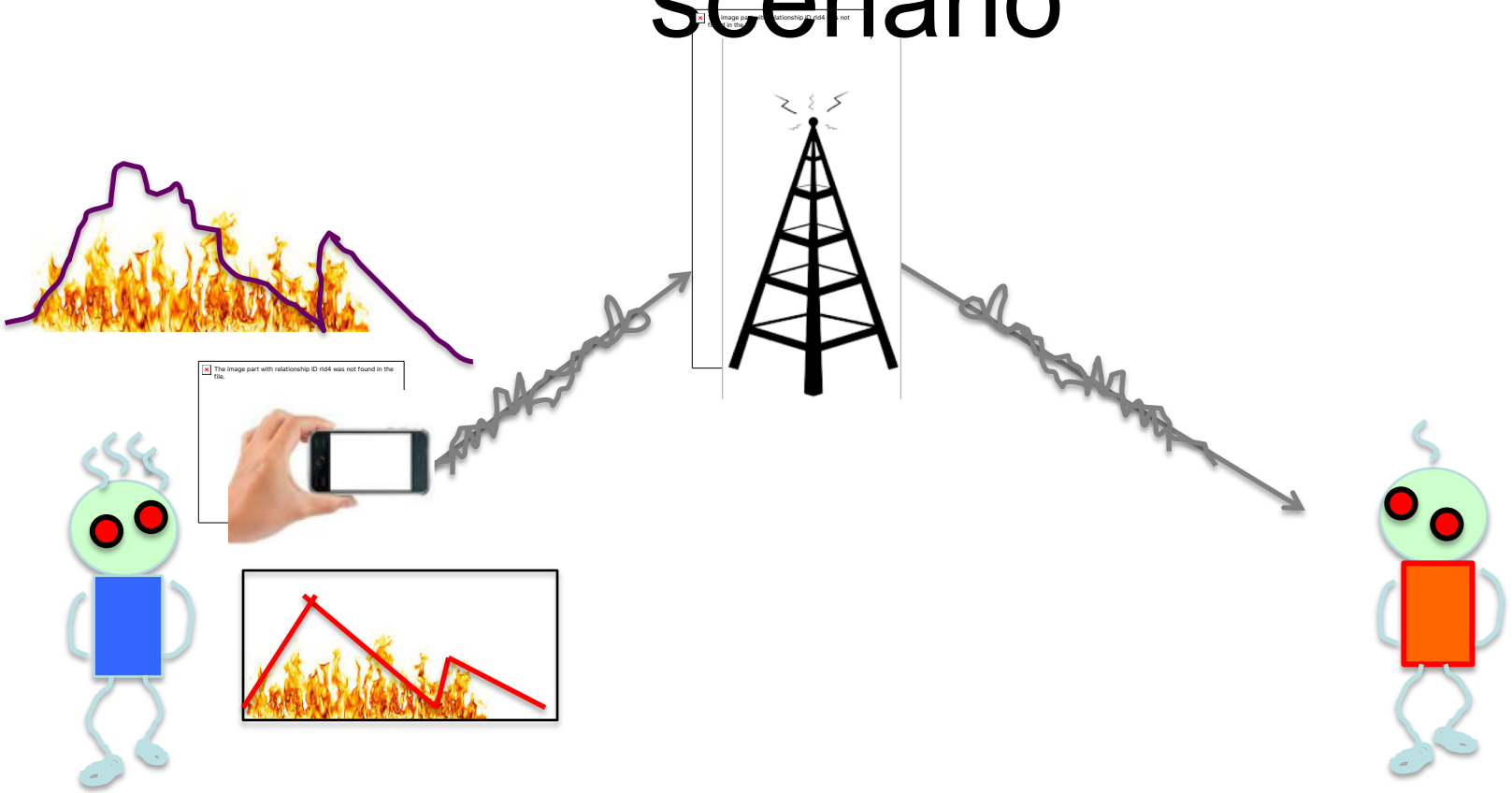
Information communication

- Communication: One “mind” affecting the other
  - Accurately transmit and reconstruct symbols (The technical problem.)
  - How precisely do the transmitted symbols convey the desired meaning? (The semantic problem.)
  - How effectively does the received meaning affect conduct in the desired way? (The effectiveness problem.)

Information theory addresses the technical problem of **reproducing the symbols.**

[1] Recent Contributions to the Mathematical Theory of Communication
Warren Weaver
https://www.panarchy.org/weaver/communication.html

Information communication scenario



- How much “information” to send? (Technical)
- How fast? (Semantic)
- How effective? (Effectiveness)

Information theory gives technical measures, tools and techniques to represent and analyze information communication.

Information communication systems

- Sensing, Processing, and Communication are universal concepts that come in many forms.

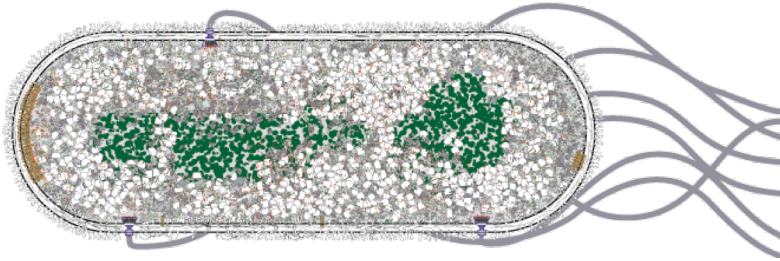
- Machine-to-machine:
  Internet of Things (IoT)

- Biological systems

Sensing, Processing & Communication

- Living organisms survive by constantly sensing, processing, and communicating information about,
  - threats and opportunities in the world around them.

Single-cell E-coli bacteria has a sophisticated Chemical sensor patch on one end (orange molecules in image below) that detect several different aspects of its environment.
Information processing machinery within single cells involves a complex network of tens or hundreds of thousands of protein mechanisms, genes and gene-expression control pathways that dynamically adapt the cell's function to its environment.



http://evolutionofcomputing.org/Multicellular/BiologicalInformationProcessing.html

Sensing, Processing & Communication

- Living organisms survive by constantly sensing, processing, and communicating information about,
  - threats and opportunities in the world around them

"Many herbal plants such as strawberry, clover, reed and ground elder naturally form networks. Individual plants remain connected with each other for a certain period of time by means of runners. These connections enable the plants to share information with each other via internal channels. They are therefore very similar to computer networks. But what do plants want to chat to each other about?

Recently Stuefer and his colleagues were the first to demonstrate that clover plants warn each other via the network links if enemies are nearby. If one of the plants is attacked by caterpillars, the other members of the network are warned via an internal signal. Once warned, the intact plants strengthen their chemical and mechanical resistance so that they are less attractive for advancing caterpillars. "

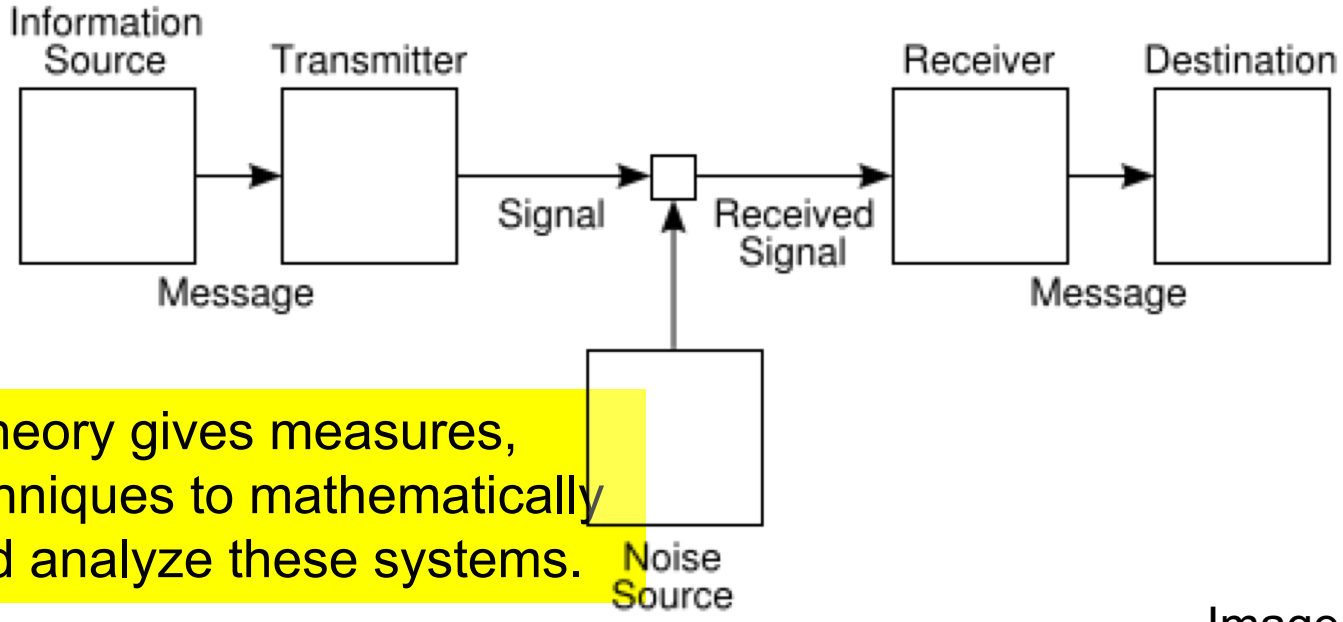
http://www.sciencedaily.com/releases/2007/09/070925095313.htm

A model for information communication

- A *model* for information communication problem.

1. Information source
2. Communication

Goal: reproduction the source output at the destination.



Information theory gives measures, tools and techniques to mathematically represent and analyze these systems.

Image: wikipedia

Shannon Theory – Turing Theory

Shannon (1916-2001)

- Information communication
  - What is possible/impossible in a setting
  - How close we can get to the limit

- Shannon's entropy: a specific type of information measure

- Other measures of information:
  - Renyi entropy
  - Algorithmic information theory (Kolmogorov)
  - ..

Turing (1912-1954)

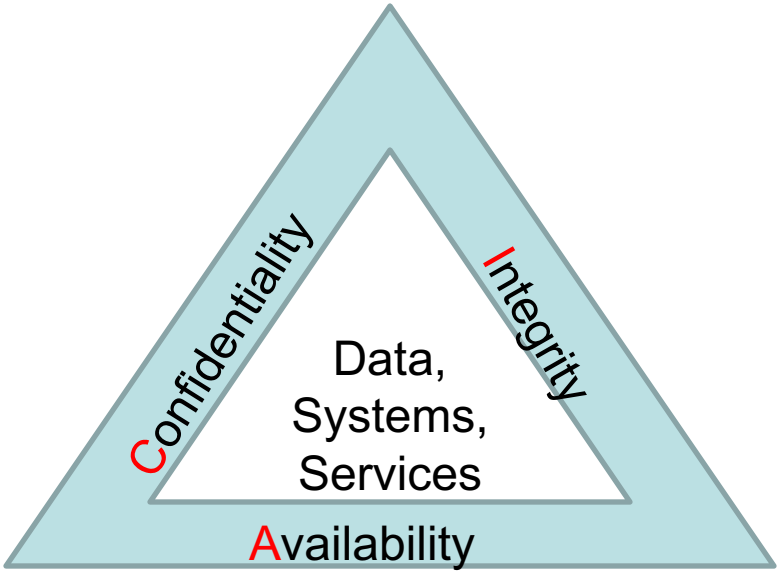
- Computation
  - What we can/cannot compute
  - How efficient

- Turing machine: a specific model of computation

- Other models of computation:
  - Quantum computers
  - Biological computers
  - ..

2. Information Security:
what do we want?

Protection against unauthorized access.



Accuracy of information.

CIA

Information is available when required.

Many facets of information security

A CSO's (Chief Security Officer) view of security:

1. Authentication and access control
2. Communication and network Security
3. Application security
4. Risk assessment
5. Business continuity and disaster recovery planning
6. Legal and compliance
7. ……

Protections

1. Legal, regulations, compliance and investigations
2. Hardware security
3. Algorithms and protocols

- All links in the chain must be strong.

Algorithms & protocols for InfoSec

- Cryptography gives a toolbox of algorithms for providing security.
  - Complemented by cryptanalysis.

- Data analysis techniques give complementary techniques for detecting malicious behavior, privacy breach..

Cryptography

- Mathematical algorithms and protocols for providing security against an adversary.
  - Formal model, security proofs

- Adversary's computational power:
  1. Computationally limited:
     - Turing computer, polynomially bounded
     - quantum computer
  2. Computationally unlimited.
     - Information theoretic

Information Theoretic Cryptography

- Adversary has unlimited computation
  - Security is because of insufficient information
  - Security will last for all future time
    - Quantum-safe

Info Theoretic & Computational

IT crypto

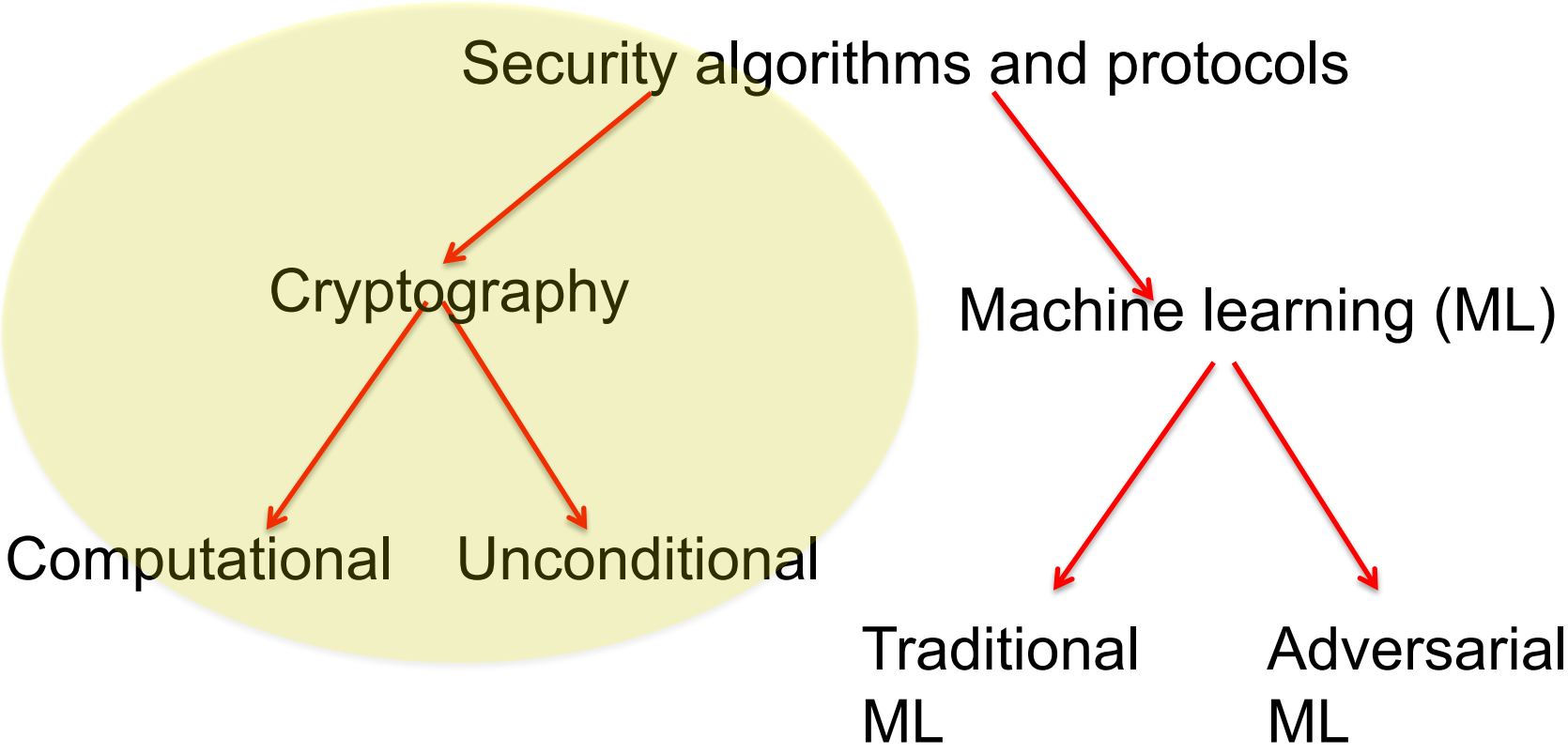
1. Protection does not change with time
   - Does not depend on computer
2. Secure in presence of a quantum computer
3. Impossible/inefficient to do certain tasks
   - Digital signature

1. Less inefficient than computational systems

Computational crypto

1. Protection has a life time
   - New computers
   - New algorithms
2. Most existing systems (e.g. TLS, RSA, DH..) will be insecure if a quantum computers exist.
3. New functionalities
   1. Impossible in IT crypto
   - Digital signature
4. Can be made efficient

Algorithms and protocols for security



This course

- Information theoretic concepts
  - Entropy of a random variable
  - Mutual information of two random variables
    - Distance and similarity
  - Encoding/decoding information source
- Information theoretic cryptography
  - Confidentiality
  - Authentication
  - Secret sharing
  - Secure message transmission?
- Information theory in security
  - Randomness and true random number generation
  - Data analysis (inferences) in security

References:

- Chapter 1: Cover-Thomas, Katz-Lindell

Other:

- http://spectrum.ieee.org/geek-life/history/celebrating-claude-shannon