Lecture 1

Lecture 1
Sunday, May 5, 2019  10:12 PM

Course: Crypt 308 - Computability & Complexity

Valentine Kabanets

About the Course:

Foundations of CS

Computer: What is it?
How powerful is it?

- Algorithms
- argue computer is powerful via efficient algorithms

- Comp/Complexity
- computers are not all-powerful
- limitations
- not computable
- not computable efficiently

A. Turing 1936
D. Hilbert 1900

Algorithms
Turing machine: model of a human computer
- finite set of states of mind
- each time, read one page
- depending on my state, contents of page,
  write such new & change my state & move to another sheet.

Power of Computers:
- computer viruses/self-replicating programs

Write a Java prog:
that will print its own source code
that will print its own source code.

. Virus detecting program? Impossible!

. Can replace mathematicians by computers? Given a statement about not numbers, \((\forall x \exists y \ y > x)\) decide if it's true. Impossible!

. Hard vs. easy problems.

\[ \text{P} \subseteq \text{NP} \subseteq \text{EXPTIME} \]

They: There exist unsolvable problems.

\[ \text{Pf.} \]

Problem: \( f: \{0,1\}^* \rightarrow \{0,1\} \)

\( f_{0,1} \)
Algorithm: Java program like natural numbers

\[ \{ \text{Java programs} \} \text{ is countable} \]

\[ f(0), f(1), f(00), f(01), \ldots \]

\[ \{ \text{funs} \} \text{ is uncountable!} \]