# Theoretical Computer Science

Devansh Shringi
(based on presentation by Sanjeev Arora)

# The algorithm-enabled economy

Google™ Deutschland

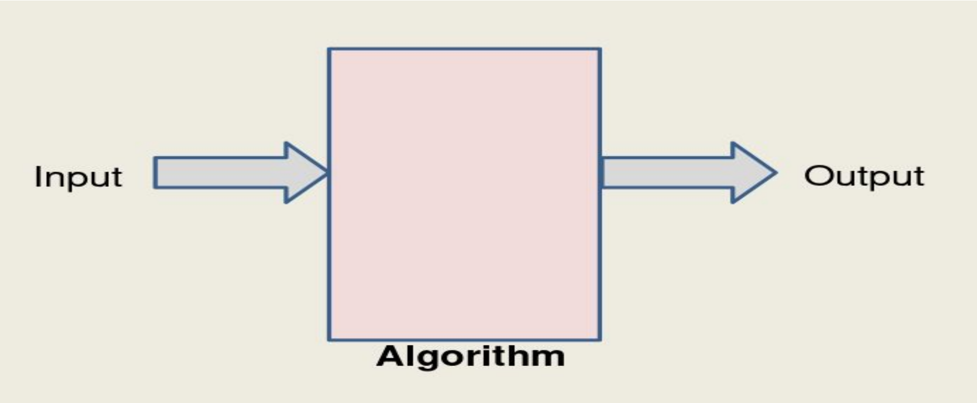
RSA SECURITY

YouTube

*What is the underlying science ?*

amazon.com

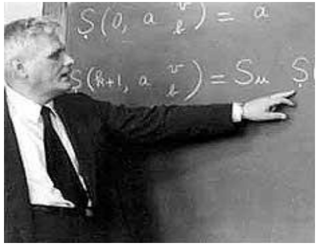
# What is an algorithm ?



# What is the computational power of physical systems?

*Church-Turing Thesis:*

Every physically realizable computation can be performed on a C program. (Or Turing machine)



Amazing Result(Turing 1936): “There are problems that cannot be solved ! (Eg. Halting)”

# Limited Resource Computation

- Time
- Space

# Assisting Algorithms

- Certificates
- Random Bits
- Advice Strings

# Algorithms for Unique Computers

- Quantum Algorithms
- Circuits - Boolean , Arithmetic
- Any system with Laws (Eg. Insects)

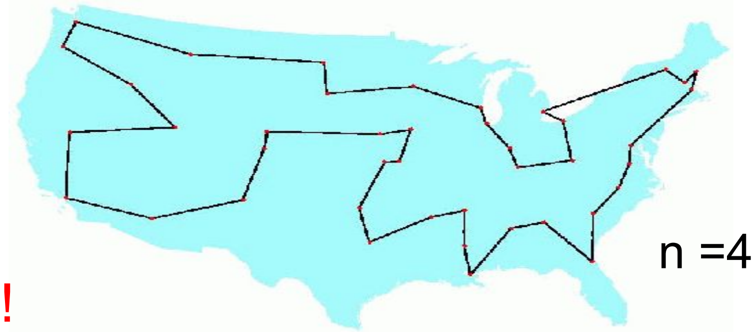
# Why ?

NECESSITY IS THE MOTHER OF INVENTION
Plato
mooskurado.com

# A central theme in modern TCS: Computational Complexity

How much time (i.e., # of basic operations) are needed to solve an instance of the problem?

Example: Traveling Salesperson Problem on n cities



n =49

Number of all possible salesman tours = n!

(> # of atoms in the universe for n =49)

One key distinction: *Polynomial time* ($n^3$, $n^7$ etc.)

versus

*Exponential time* ($2^n$, n!, etc.)

# If P = NP, then brilliance will become routine

- Proofs of Math Theorems can be found in time polynomial in the proof length
- Patterns in experimental data can be found in time polynomial in the length of the pattern.
- All current cryptosystems compromised.
- Many AI problems have efficient algorithms.

# TCS @ IITK
# Primes in P

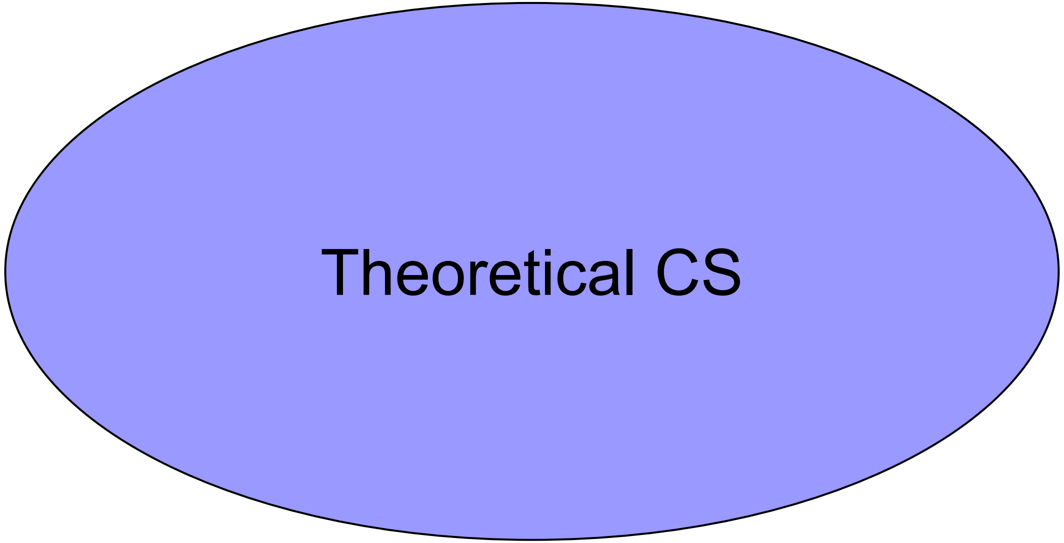
- Given a number n finding if it is prime or not in polynomial time wrt to number of digits
- Basic question in maths and computer science
- AKS algorithm
- Using algebra and PIT
- Won the Godel Prize

# How to Start ?

- It’s Tough, as all things worth doing are
- Find interest through DCs
- Do Graduate Courses
- Find a problem you want to solve
- Work with a Prof in field

# Questions ?

Hope you will be expanding this in the years to come!


Theoretical CS

Thank You