How has Computing Changed the World?

A Panel Discussion

Tue, 17 Jan 2012 at 7pm EST

Hartley Room at Florida Tech

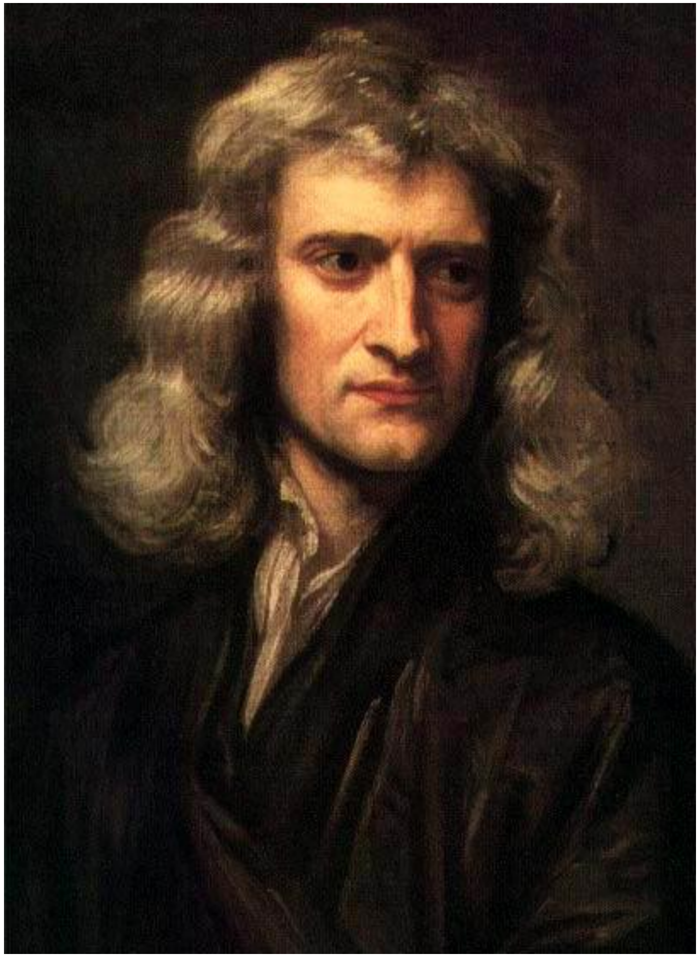
Dr. Ryan Stansifer

- Dr. Ryan Stansifer is an Associate Professor in the Department of Computer Sciences at the Florida Institute of Technology. He joined the faculty in 1995. He has a Ph.D. from Cornell University.
- His research interests are in programming languages, especially type theory and functional language. He hopes to strength problem solving abilities in his students through intercollegiate programming competitions.

Physics: Barnes-Hut

Ryan Stansifer

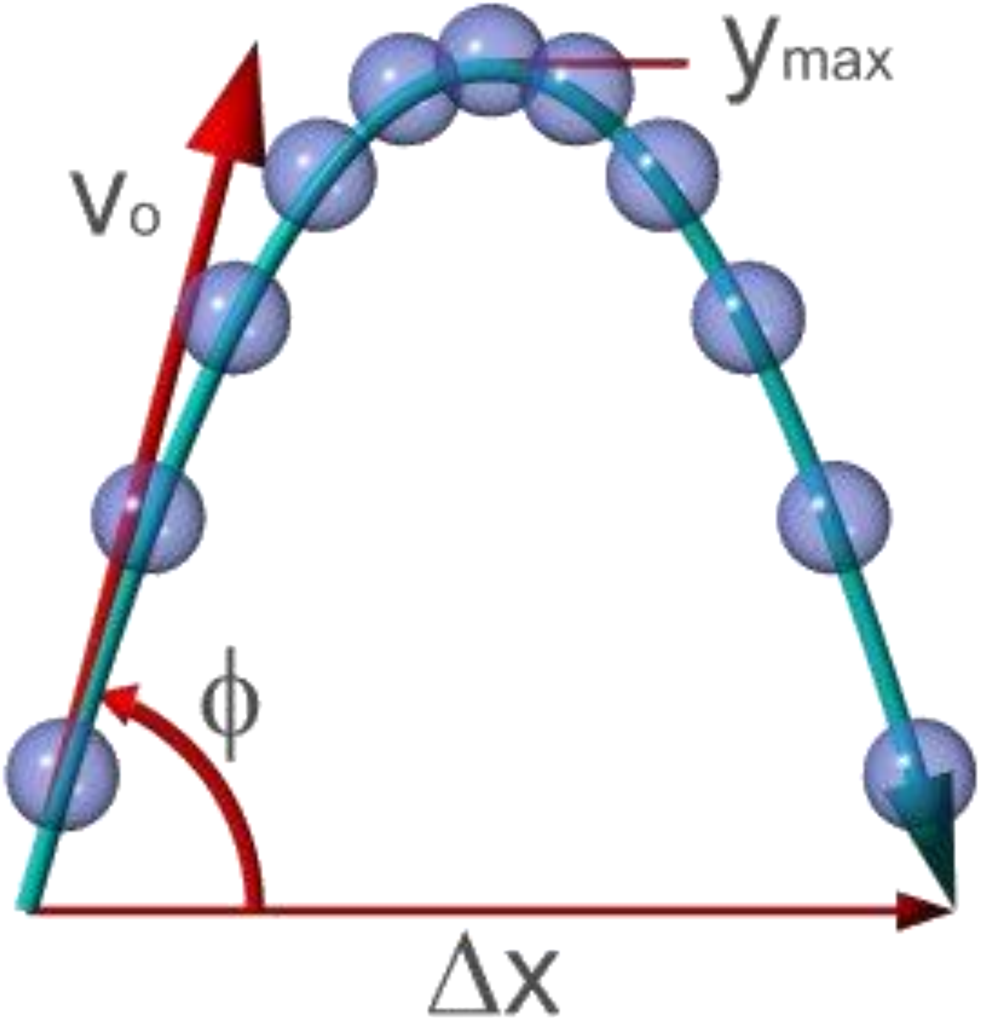
Isaac Newton



- Although Newton’s laws of motion explain the motion of everything in the universe, there is a problem.

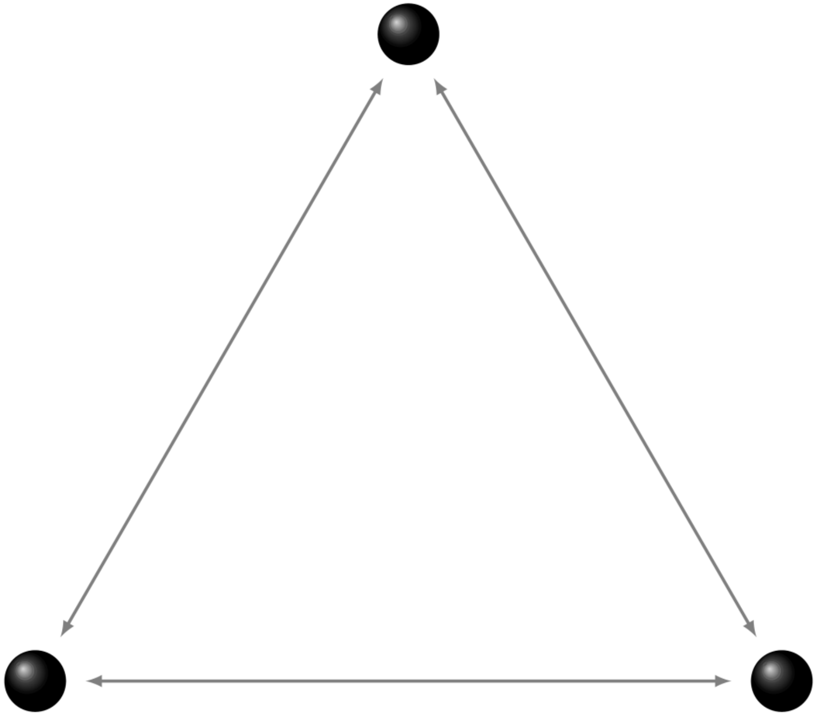
- Classical mechanics is completely deterministic: Given the exact positions and velocities of all particles at a given time, one can calculate the future (and past) positions and velocities of all particles at any other time.

Classical Mechanics

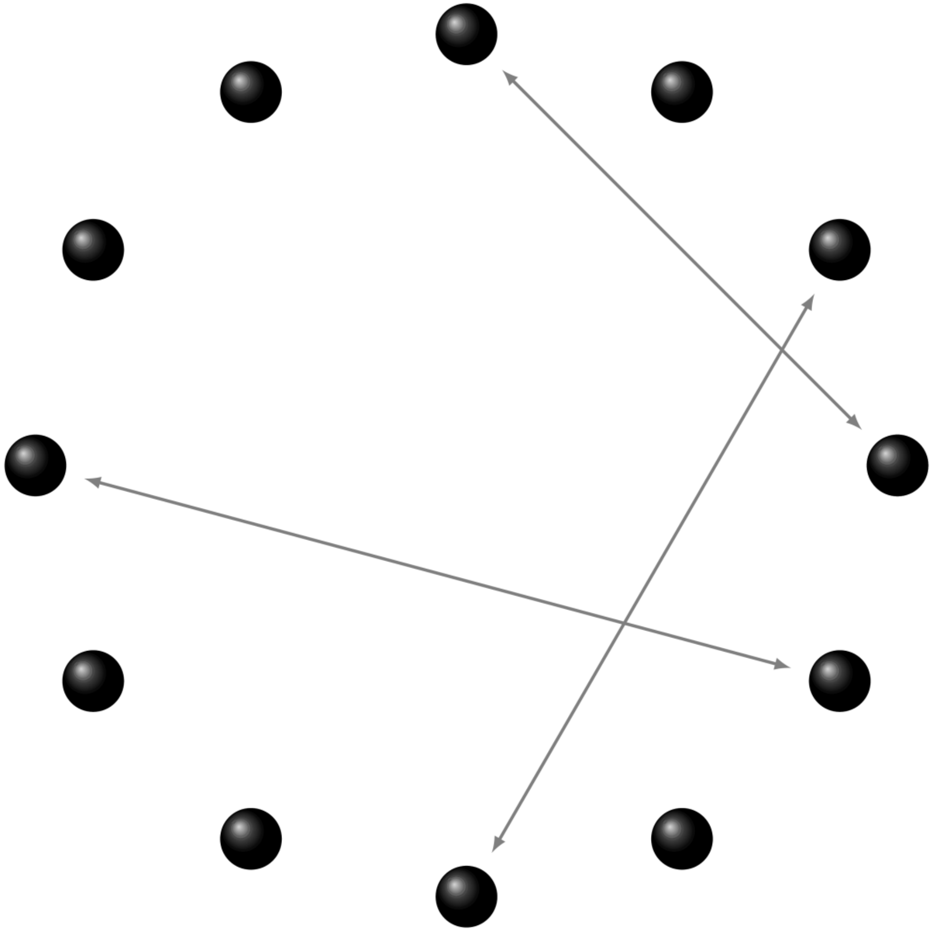


Two Body Problem Is Solved

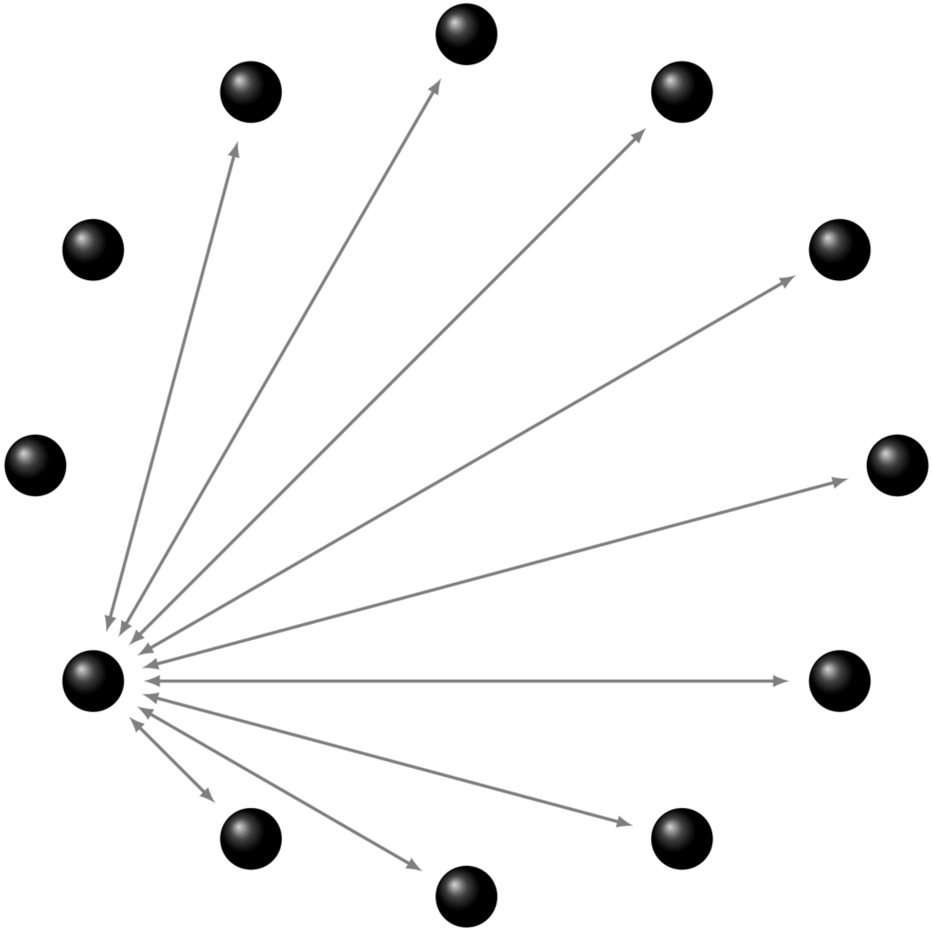
Three Body Problem Has No Solution



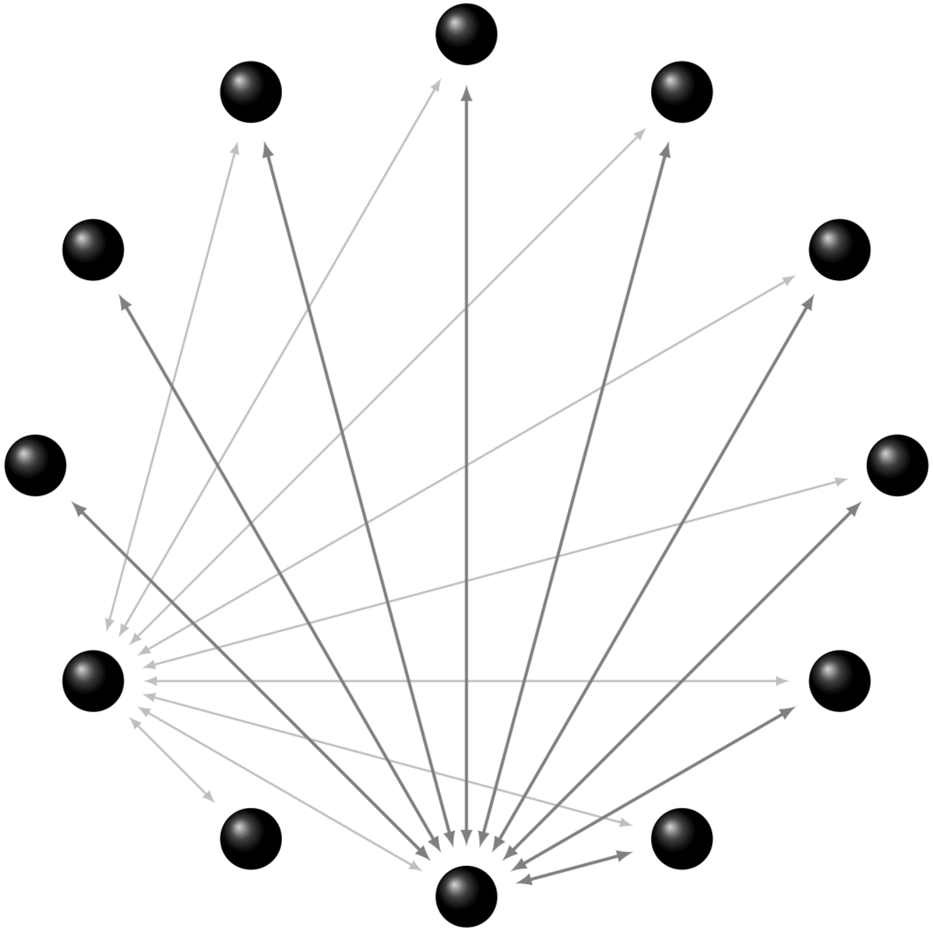
Computers Can Solve Numerically



But There Are …

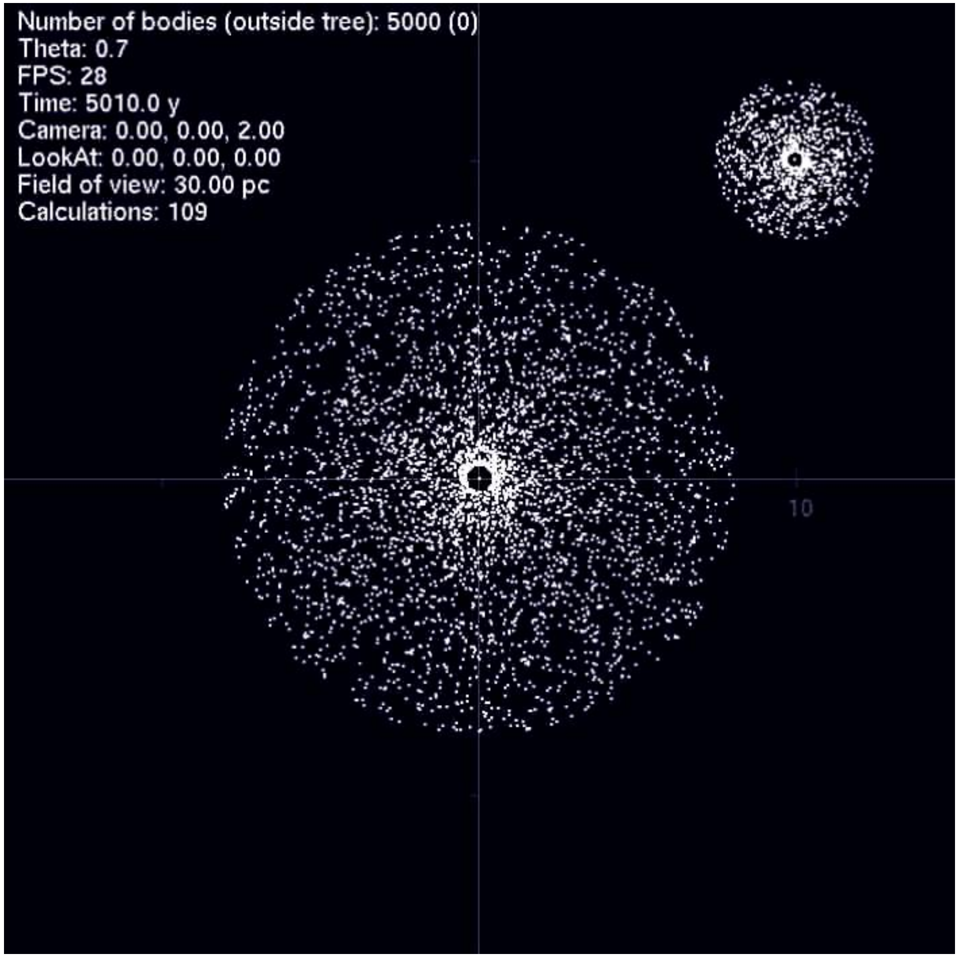


Just Too Many Interactions



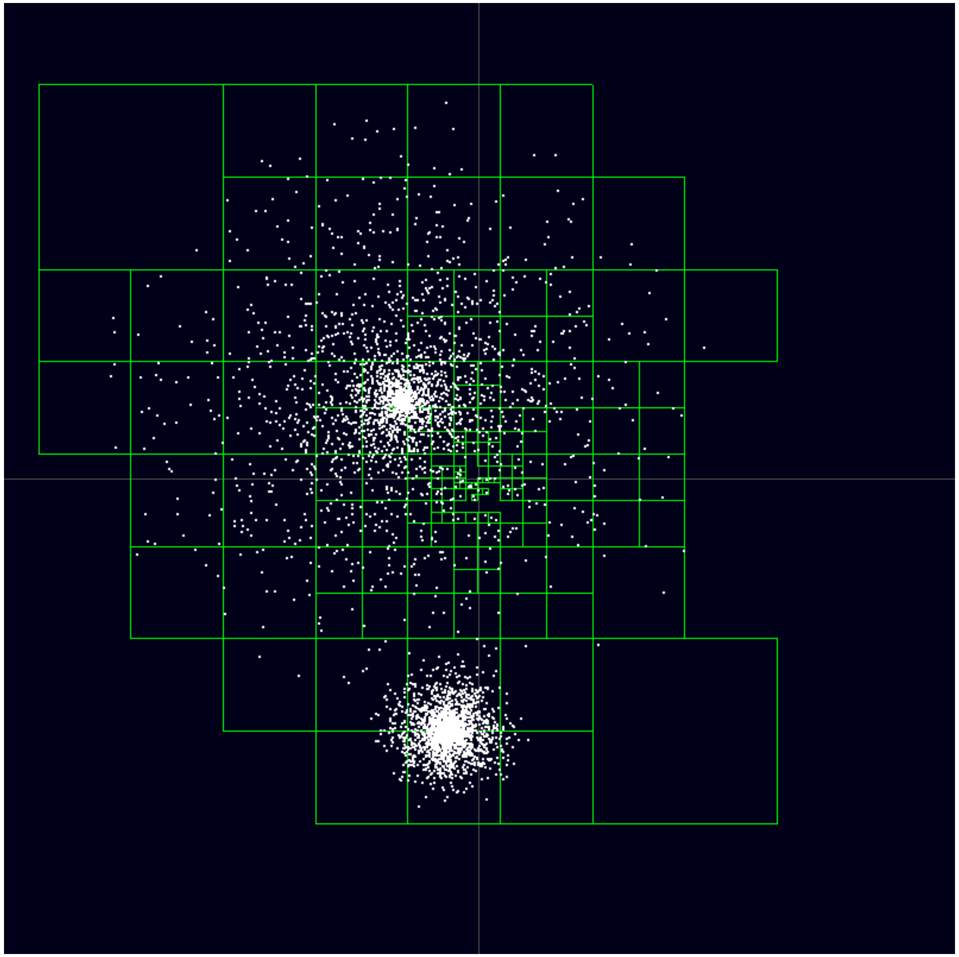
Computer Science

- Invents an algorithm to efficiently deal with the many interactions by using a clever way of dividing up the universe unto unequal regions.
- There result is science that was otherwise not possible



Number of bodies (outside tree): 5000 (0)
Theta: 0.7
FPS: 28
Time: 5010.0 y
Camera: 0.00, 0.00, 2.00
LookAt: 0.00, 0.00, 0.00
Field of view: 30.00 pc
Calculations: 109

Barnes-Hut Uses Octrees



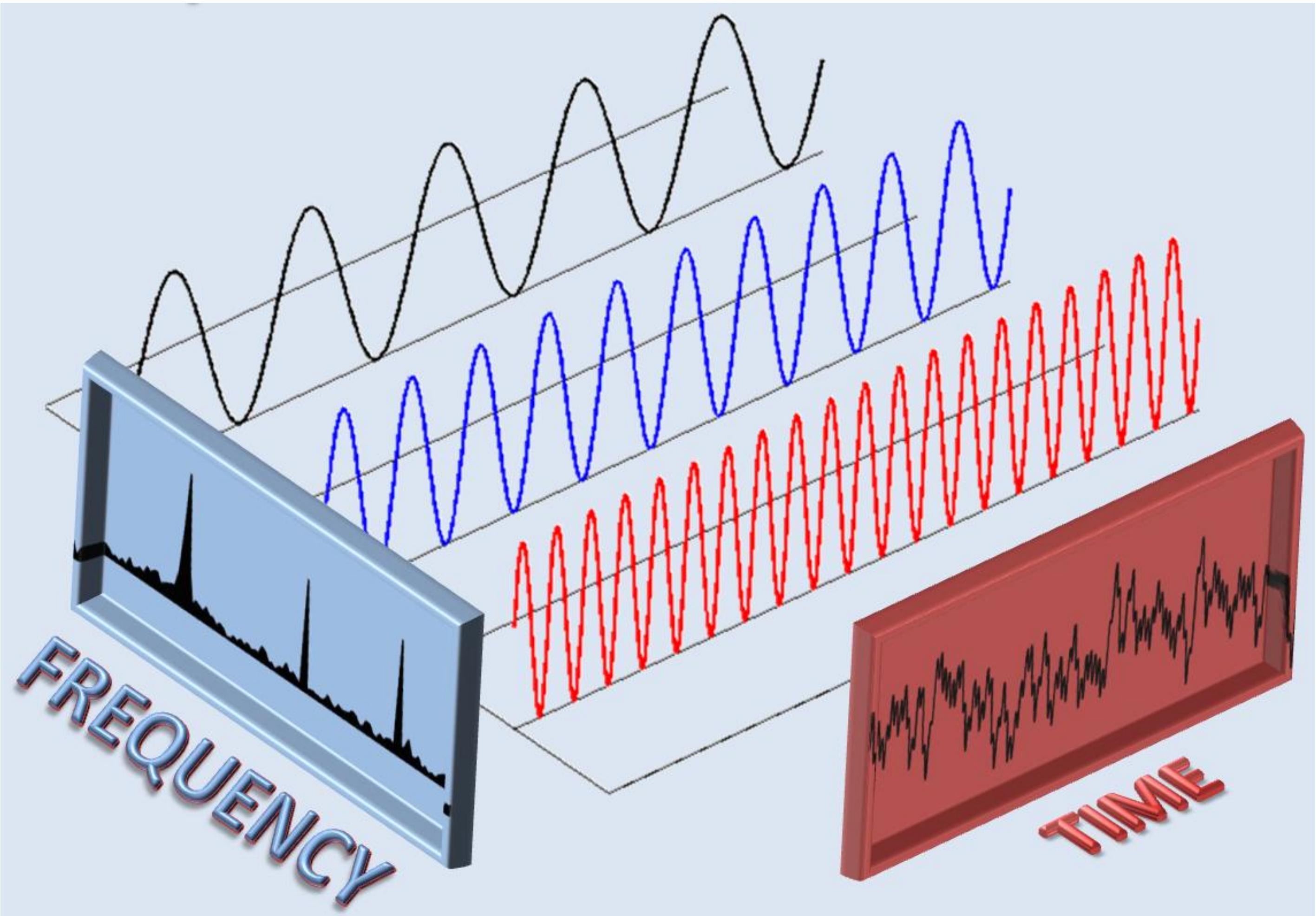
- “N-body simulations are simple in principle, because they merely involve integrating the 6N ordinary differential equations defining the particle motions in Newtonian gravity. In practice, the number N of particles involved is usually very large (typical simulations include many millions, the Millennium simulation includes ten billion) and the number of particle-particle interactions needing to be computed increases as N^2, and so ordinary methods of integrating numerical differential equations, such as the Runge-Kutta method, are inadequate.” Wikipedia

Fast Fourier Transform

Ryan Stansifer

Carl Friedrich Gauβ

- The Fourier transform is a mathematical method for transforming a function of time into a function of frequency. It is useful for analysis of time-dependent phenomena, for example the analysis of sound. It is important to assess the frequency distribution of the power in a sound because the human ear exercises that capacity in the hearing process.


FREQUENCY
TIME

Speech recognition, MRI, digital camera (JPG)

AT&T
11:34 AM
90%
“Find me a French restaurant in Bethesda Maryland”
I found 13 French restaurants... 7 of them are in Bethesda.
Woodmont Avenue
Mon Ami Gabi
171 reviews
Old Georgetown Road
La Madeleine French Bakery & Cafe
53 reviews
Fairmont Avenue

- The signals that we measure in MRI are a combination of signals from all over the object being imaged. The Fourier transform allows us to work out what those frequencies and amplitudes are.

Cooley–Tukey algorithm
Fast Fourier Transform

- Just like the n-body problem, too many interactions to be practical for application to large problems
- Cooley-Tukey algorithm: a divide and conquer algorithm that recursively decomposes the problem into many smaller pieces
- The algorithm is fast enough to enable new technology.

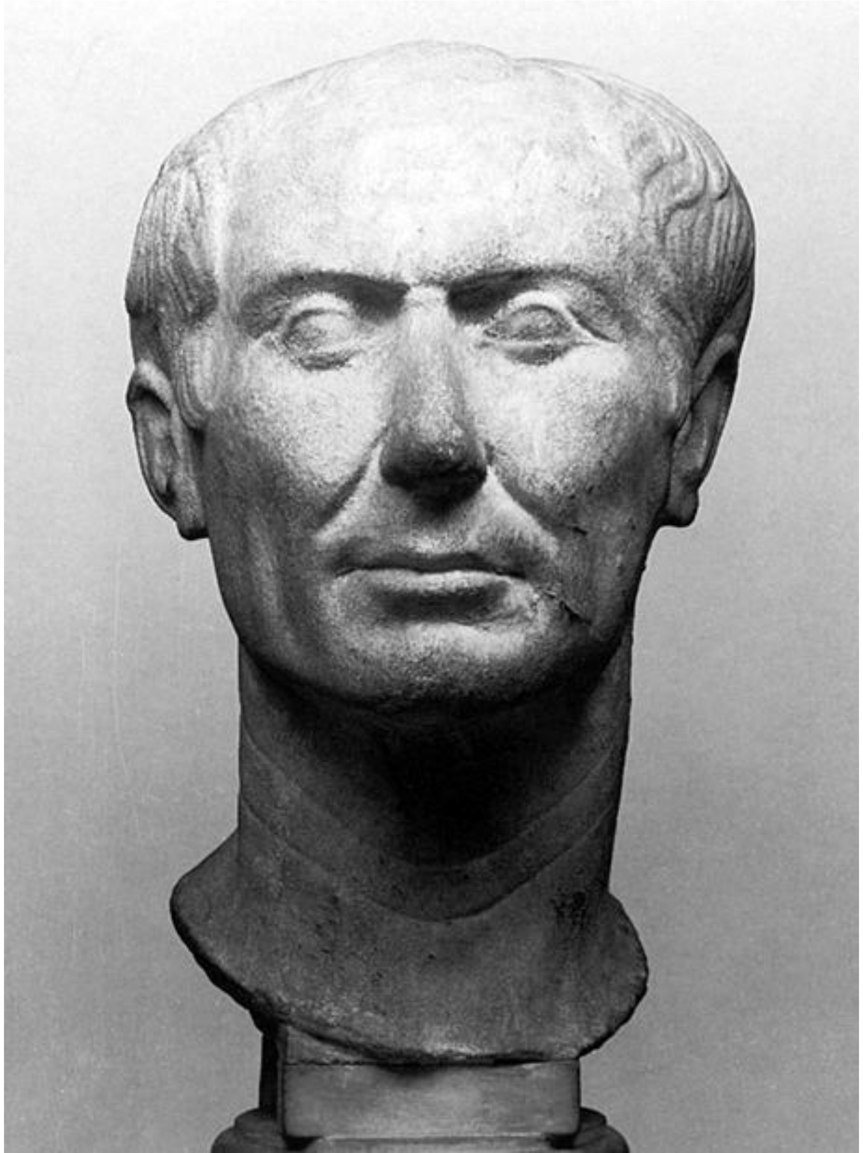
Brief Analogy With Multiplication

- Compare two ways of multiplying: n*n*n*n*n*n*n*n= n^8
- Or: n*n=m; m*m=p; p*p=n^8. Only three multiplications

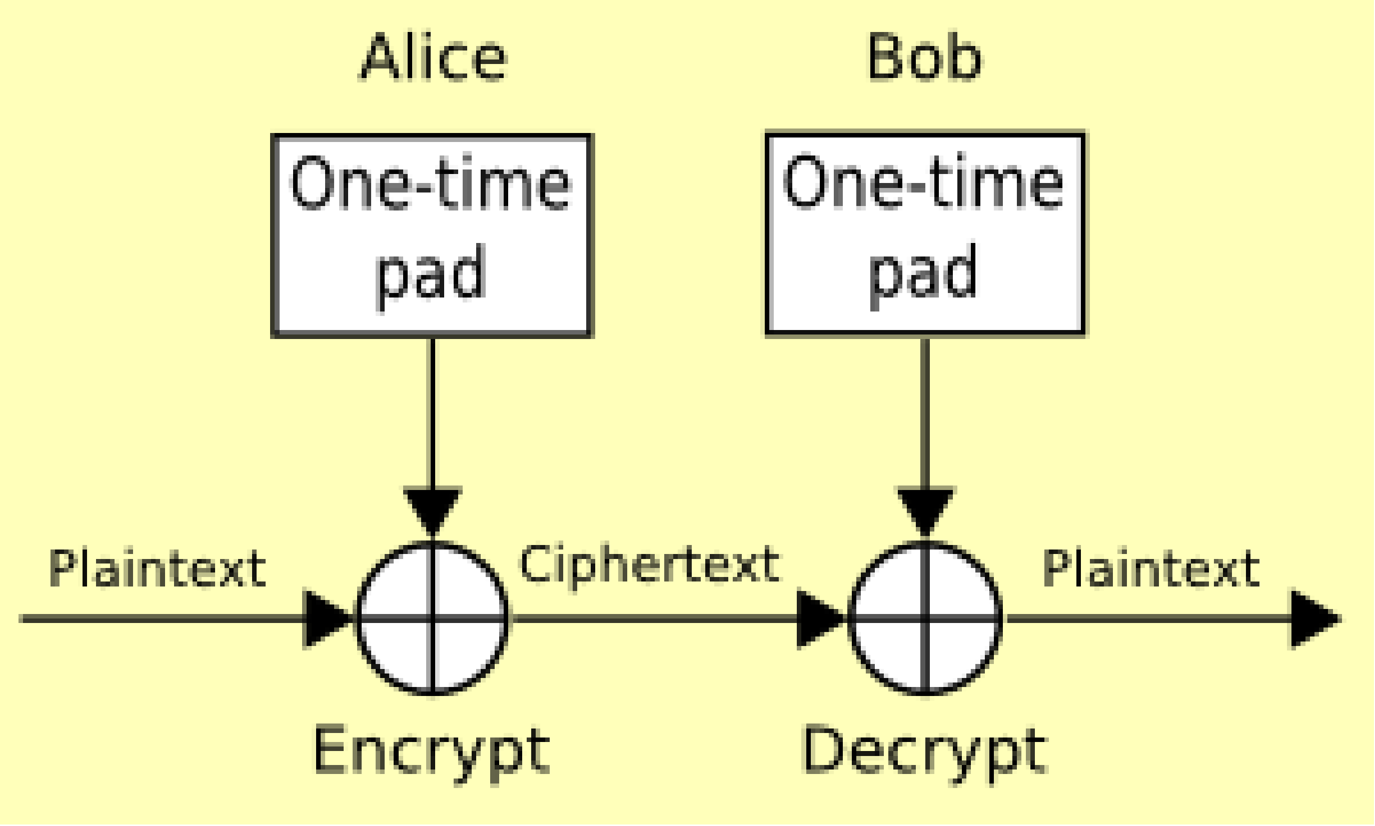
Secure Protocols

Ryan Stansifer

Julius Caesar



- Computer Science (sometimes known as Informatics) is about information and protocols
- There are some amazing ones with far reaching applications:
  - Cryptography
  - Auctions
  - Zero -knowledge proofs


Alice
Bob
One-time pad
One-time pad
Plaintext
Ciphertext
Plaintext
Encrypt
Decrypt

One-Time Pad

- One-time pads have been known for hundreds of years
- The science of information can prove that a one-time pad is a *perfectly* secure means of communication.
- But it requires a shared key. If you can share a secure key perfectly, why do you need a one-time pad?
- Not unreasonable, that security should come with a cost.

- In fact, perfect encryption is possible with *no covert channel necessary*
- Stunning!
- The key? Public-key encryption
- Enables: e-commerce

BTW

- Security is a multifaceted problem.
- Perfect security in an information sense does not prevent mischief in a complex world
- Authentication, man-in-the-middle attacks, replay, protocol compatibility, “fall-back”, etc
- No one is going to “break” public-key encryption as a practical matter, but there is legitimate concern about exploits to its use.

Bit Commitment

A commitment scheme allows one to commit to a value while keeping it hidden, with the ability to reveal the committed value later. Commitments are used to bind a party to a value so that they cannot adapt to other messages in order to gain some kind of inappropriate advantage. They are important to a variety of cryptographic protocols including secure coin flipping and zero-knowledge proofs.

Coin flipping

Suppose Alice and Bob want to resolve some dilemma via coin flipping. If they are physically in the same place, a typical procedure might be:

1. Bob "calls" the coin flip
2. Alice flips the coin
3. If Bob's call is correct, he wins.

Suppose, however, they are in different rooms and so Bob can not see Alice tossing the coin. If they do not trust one another, then they need a way to ensure that Bob does not change his call when he hears the result, nor Alice change the reported result when she knows Bob’s guess.

One way to do this is for Bob to write down his guess and put it in a sealed envelope, which he gives to Alice. Then Alice tosses the coin and reports the result. Together they open the envelope and see if Bob’s guess was correct. This is called a *commit and reveal* process. Bob commits his guess to paper and then, after Alice has announced the result, he reveals it to Alice.

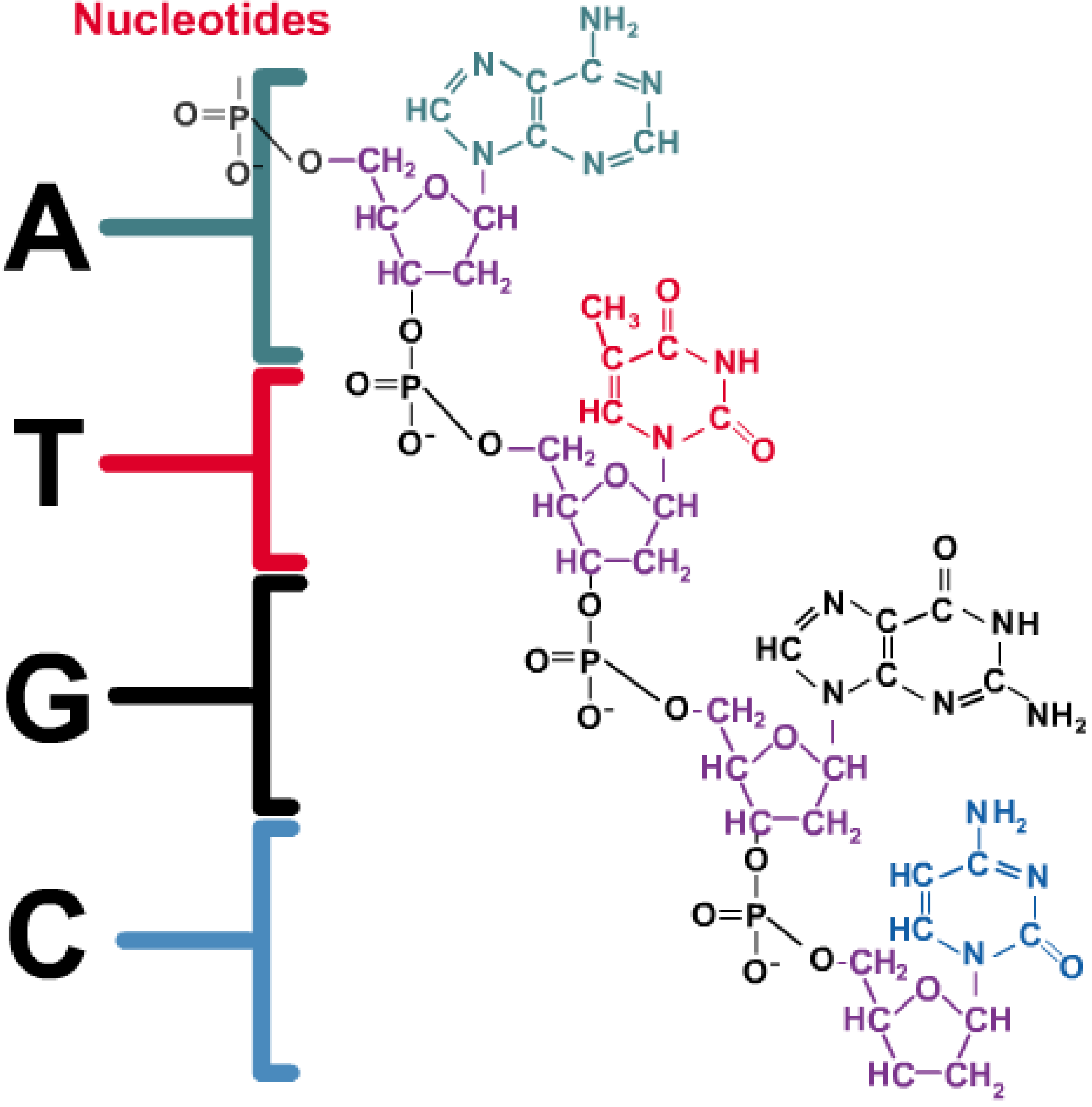
- Amazing, this is possible because of “trap-door” functions – functions that easy to compute in one way, but the inverse is hard.
- So suppose Alice and Bob agree that odd=heads. Then Bob commits f(x)=y for some random x (either odd or even). After the flip Bob gives Alice x and she can verify that f(x)=y. Bob cannot renege his original commitment.

DNA Sequencing

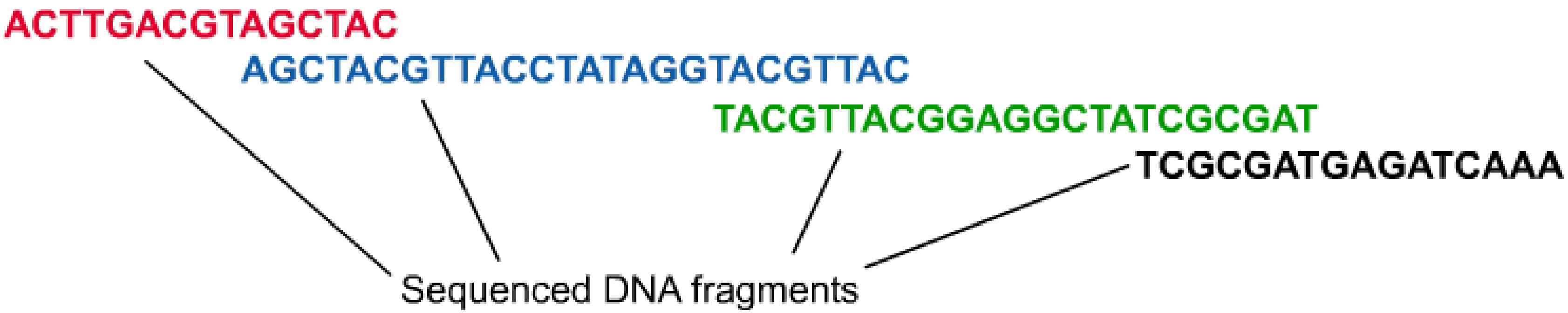
Ryan Stansifer

Watson and Crick

Nucleotides



Shortest Common Supersequence



ACTTGACGTAGCTAC

AGCTACGTTACCTATAGGTACGTTAC

TACGTTACGGAGGCTATCGCGAT

TCGCGATGAGATCAAA

Sequenced DNA fragments

In Conclusion

- Public policy challenge
- http://www.youtube.com/watch?v=063JN4h06eI
- Rep. Jared Polis, Computer Science Education Week remarks.