Assignment 05: Socketing

Brock Davis

Computer Programming III

May 2017

Goal

- Use socketing to perform computationally heavy tasks
- Build a Server class and Client class
  - Single Server to relegate tasks to multiple Clients
- Task: Factoring Semiprimes
  - Product of 2 primes

Approach Overview

- Server gives prime and range of indexes to test
- Server command
  - SOLVE [NUM] [STARTN] [STOPN]
- Client responses
  - CRACKED [FACTOR1] [FACTOR2]
  - FAILED
- Iterating quadratic equations to factor semiprimes

Factoring Approach

$$N \equiv semiprime \qquad p, q \, \epsilon \, \mathbb{P} \qquad 2n = p + q$$

$$2n = p + \frac{N}{p} \qquad\qquad 0 = p^2 - 2np + N$$

$$p = n \pm \sqrt{n^2 - N} \qquad for\ some\ n,\ \sqrt{N} < n < N$$

$n + \sqrt{n^2 - N}$ is a whole number for only one n, and that whole number is p.

- n is iterated from sqrt(N) to N until a whole number is found

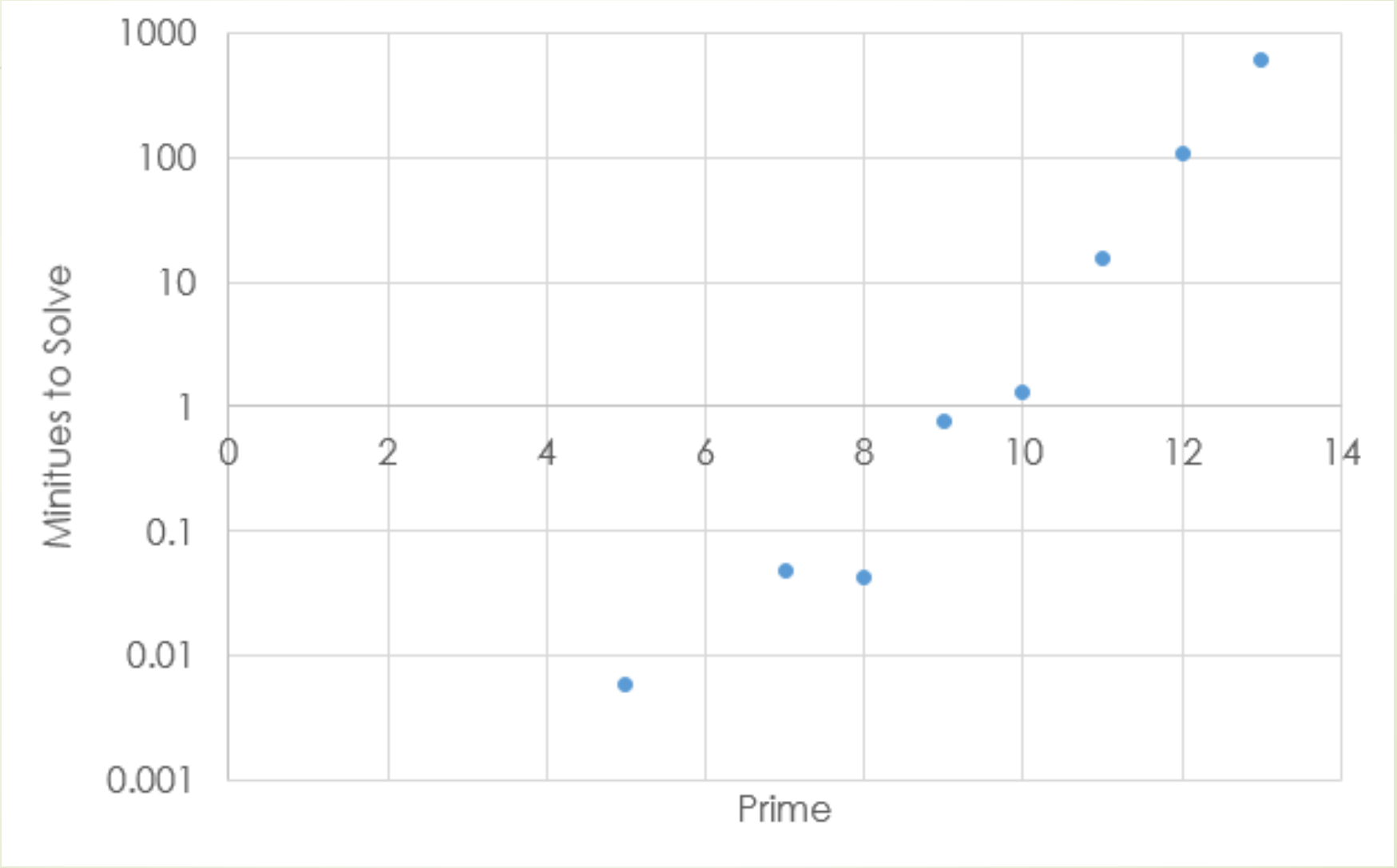
Server Overview

- Reads in semiprimes, calculates sqrt(N), (starting point) stores them for solving
- Assigns each Client the current N to factor, and a range of 10 million n's to check
- Continues assigning consecutive n's until factorization is found
- Logs time and events:
  - Connect/disconnect
  - Task assigned
  - Cracked number
  - Progress made

Results

- After 12 hours, a total of 14 semiprimes were cracked.
  - 2 digits up to 25 digits
- The time to crack each semiprime increased exponentiallly

Time To Factor



Future Improvements

- Faster semiprime factoring algorithm
  - Quadratic Sieve method
- More sockets
  - Utilize more computers