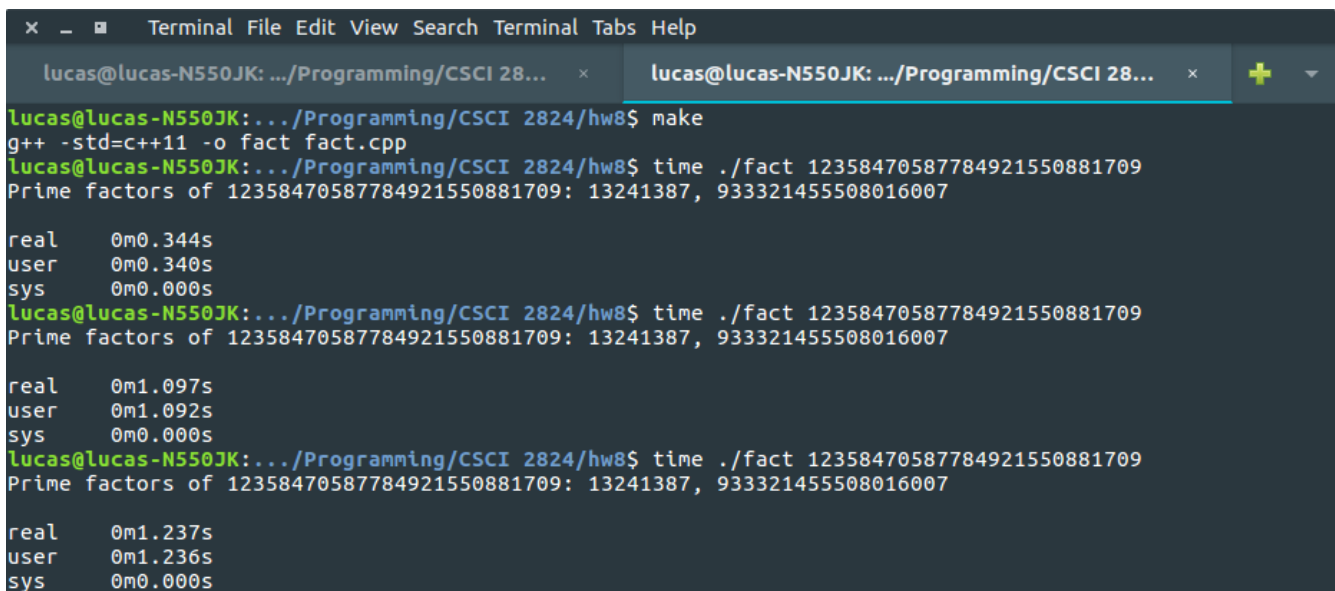


Homework 8: Prime Factorization

This program uses Pollard's Rho Algorithm to find prime factors p and q such that $p \cdot q = N$ where N is composite. Pollard's Rho Algorithm uses the fact that the probability of picking two equal random numbers from a list of t random numbers from 1 to N is 50% if $t > 1.177N^{1/2}$. Similarly, we will have the same probability of finding two numbers whose difference is a factor of N . More generally, $\text{GCD}(x_1 - x_2, N) = p$. The algorithm uses a pseudo random sequence, $f(x) = x \cdot x + \text{seed} \bmod N$ where the seed changes when a cycle has been detected. The program uses Floyd's cycle-finding algorithm to detect repetition. On each loop, a is set to $f(a)$ and b is set to $f(f(a))$. When $f(a) = f(f(a))$, a cycle has been detected and the seed in $f(x)$ is changed.

How To Run

First compile with 'make'. Then run './fact <number>'. Running './fact' with no arguments outputs a usage message.



```
lucas@lucas-N550JK: .../Programming/CSCI 28... x lucas@lucas-N550JK: .../Programming/CSCI 28... x +
lucas@lucas-N550JK: .../Programming/CSCI 2824/hw8$ make
g++ -std=c++11 -o fact fact.cpp
lucas@lucas-N550JK: .../Programming/CSCI 2824/hw8$ time ./fact 12358470587784921550881709
Prime factors of 12358470587784921550881709: 13241387, 933321455508016007

real    0m0.344s
user    0m0.340s
sys     0m0.000s
lucas@lucas-N550JK: .../Programming/CSCI 2824/hw8$ time ./fact 12358470587784921550881709
Prime factors of 12358470587784921550881709: 13241387, 933321455508016007

real    0m1.097s
user    0m1.092s
sys     0m0.000s
lucas@lucas-N550JK: .../Programming/CSCI 2824/hw8$ time ./fact 12358470587784921550881709
Prime factors of 12358470587784921550881709: 13241387, 933321455508016007

real    0m1.237s
user    0m1.236s
sys     0m0.000s
```