Daniel Carlson, Nadine Garcia, Lindsey Mantell
CSCI5471
Contribution

Contributions:

All three parties spent time together reading and discussing the paper. We all met up for anywhere from 2-3 hours from the 10 weeks ranging from February 24th to April 28th which computer to about an average of 25 hours spent together working on our project. Tasks we accomplished together include collection methods of keys, classification of keys, analysis of attacks, and distribution of implementation of attacks.

Individually we split the analysis up into three separate parts. Daniel Carlson handled Lehman's, Fermat's, and Batch GCD of the keys. Nadine Garcia handled Cycling Attacks, Epileptic Curves, and Quadratic Sieve. Lindsey Mantell handled Pollard's, Attacks on small private exponents, and Number Field Sieve. Analysis of these attacks consisted of writing implementations of them then group discussions on what attacks could potentially be improved with the known features of p and q. Overall, individual work on writing these programs and analyzing the data was anywhere from 15-20 hours of work. Since our keys were of length 1024 and 2048, actually factorization with results will not happen, but discussion of how these attacks work and potential improvements with the new data was a focal point.

Writing the paper and making various graphs within the paper took place over the week of April 23rd to May 1st. We spent anywhere around 10 hours both individually and together writing, proof reading, and editing the paper in a Google document format.

Overall, we each individually contributed about 50-70 hours worth of work into the paper, not including meets held with the professor and any in class discussions we had with each other.