CSE 13S Assignment 5 - Public Key Cryptography

Jaren Kawai - jkawai

How was the code tested?

The code in the source files was tested as an entire process by passing in simple messages such as hello and test. If the returned value was the same as what was originally passed in, the encryption and decryption process was successful. In addition, each of the getopt options were tested for each file by running multiple tests to see if calculations were carried out correctly, and if output messages were formatted properly.

What was learned from this assignment?

From this assignment, I learned a lot more about what it means to encrypt and decrypt data, and why it is so important to protecting some of our most sensitive data and information, Encryption and decryption were processes I had simply heard about before, but never really understood how they played a part in actually protecting information. I also learned about RSA for the first time, and doing the assignment gives me a better idea of what actually happened when I made a key pair at the beginning of the course.

In addition, I learned how to use the gmp library, and had to get used to lots of void return type functions to set variables and carry out operations which usually are much different compared to other assignments. I also learned how to deal with files and how to read and write information to and from them, which was something that I had done little with in Python, but got more of a chance to explore in this class and this assignment.

Lastly, this assignment taught me something which was less related to actual coding, but rather a practice for computer science related problems in general. I found myself generally over-complicating things, and the way I was writing functions was much harder than I was supposed to be early on. Going to sections and listening to TAs and tutors give tips made the assignment much easier, because I got around my tendency to overcomplicate problems that had rather simple solutions.