WRITEUP ASGN5

Cruzid: acristea

February 2023 - CSE13S

1 Harnessing Skills

What follows is not so much what I learned, but what I improved upon. For example, similar to our last assignment, Game of Life, we had to use multiple different files and set specific files to NULL if they were stdin or stdout by default. This also meant building three new test cases and getting lots of practice with main(). We had to allocate memory for our blocks for which we encrypt and decrypt, meaning more practice in my case using calloc(). Allocating memory came with some issues at first because I was at risk of creating segmentation faults if I accessed poor memory. Files played a big role in this assignment and I was able to confidently use my prior knowledge from assignment 4 to complete the tasks involved with no issues. One new thing I did was dealing with hex strings and their importance in encryption. At one point I forgot to write one of my variables as a hex string, formatting it as an mpz-t instead. I found it interesting how it didn't show an error compiling, so I got stuck on it for a while. Speaking of debugging, this assignment help me increase my skills significantly whenever I encountered segmentation faults.

2 GNU Arithmetic Library

Due to us having to use the mpz-t type, we had to learn how to use the GNU library. This consisted of an entire new method to add, subtract, multiply, and divide, using modulus and comparing numbers. I can see why it's useful when dealing with large amounts of data because of how many functions gmp contains. An example is gmp division and the amount of different functions offered such as floor and ceiling division and remainders. We had to use these to implement numtheory.c and throughout ss.c. It reminded me of assembly in terms of structure. After looking through the manual and seeing what was possible it was easy to get the hang of.

3 Cryptography's use in the Real World

Before starting this assignment, I did not know much about cryptography or it's use in the real world. After completing this assignment, I was curious to see how many uses cryptography had and was surprised by its versatility. For example, Venmo uses data encryption to protect us and guard us against unauthorized transactions and access to our personal or financial information. Our financial information is encrypted, stored, and protected on secure servers. Venmo is an app I use a lot, and I didn't understand how it's security worked until now. Another use of cryptography is the use of HTTPS to secure communications over a network. Any competent business with a website or mobile app for communicating with customers should be using HTTPS. Its port, number 443, is protected by an encryption algorithm, and again protects sensitive information. Back then, the usage of cryptography took a more classical form where it was specifically confined to the art of designing and breaking encryption schemes. Today, cryptography is concerned with the rigorous analysis of any system which should withstand malicious attempts to abuse it. It would be interesting to see how it will continue to change in the future.

4 Conclusion

In conclusion, this assignment taught me a lot about the functionality of cryptography, specifically speaking the ss encryption, and its applications in everyday life. In terms of my C coding knowledge, I have been able to hone and master certain skills such as debugging and becoming flexible to other arithmetic libraries/applications that can be added to my code.