Schmidt-Samoa Encryption and Decryption

Alexander Ragland #1858717

February 21, 2023

1 MP Bignum Library

In order to have adequate integer precision for the project, the MP Bignum library was mandatory. It includes many useful functions that make doing math with big numbers efficient and accurate. In particular, the integer comparison, bit count, and random functions were integral. The import and export functions, although a bit confusing at first, were also handy. Unfortunately, the library's syntax is somewhat unwieldy and lends itself to cluttered code. I refactored the code I wrote more often than usual, in order to debug the various MP function calls.

2 File I/O

Prior to this assignment, my coding skills in terms of reading and writing files was subpar. In the file encryption and decryption functions, I attempted and failed to write them without reading the fscan/fread functions' manual pages. It was only after thorough re-examination and several Youtube videos that I was able to successfully implement them. I'm much more confident now on reading from and writing to files.

3 Error Handling and System Calls

During my research on file I/O, I realized that error handling was something I should take more seriously and opt to use "proper" techniques and idioms. Besides checking that the files I was opening were valid, I also used system calls to send debugging output to stderr. System calls were also intrinsic to implementing the open and fchmod functions. I learned about using file descriptors, in order to alter file permissions.

4 Parsing Strings

Parsing strings was another topic that went hand in hand with file I/O. In order to have default file names, as well as allow inputted file names, I had to use the snprintf and memset functions. I used these functions in tandem with a buffer to store, and then later use strings to open files.

5 Reflection on Cryptography

Some interesting applications for asymmetric public-private key cryptography include encrypted email, SSL, and cryptocurrencies. Encrypted email makes uses of a public key to encrypt the contents of an email, and then uses a private key to decrypt the contents. SSL uses cryptography to securely link websites and browsers. Cryptocurrencies rely on ledgers with public keys to confirm the identity of private key holders. All of these applications provide the user with more security than traditional methods such as alphanumeric passwords.

They are also unique from symmetric cryptography based applications because there are two unique keys which each serve their own purpose, rather than one key. The most obvious way in which I use cryptography in my life is via SSH with gitLab. With it, I can create a secure connection from my local machine to a remote server. Going into the future, keeping personal information secure will be more important than ever; large companies already harvest and trade user data, and they certainly do not have the user's best interests in mind.

6 References

- Varun Golusupudi was extremely helpful to me when I was implementing the Miller-Rabin primality test, using MP library functions.
- Various users from the discord, Ben Grant in particular, were also extremely helpful in understanding general concepts and understanding the specifications in a more practical way.