From Top Secret to Top Cipher: The Schmidt-Samoa Cryptography Innovation

Lucais Sanderson

February 26, 2023

1 Introduction

Schmidt-Samoa (SS) is an encryption algorithm that uses public-key or asymmetric cryptography. Asymmetric cryptography comprises a public key, known to all, and the private key which only the owner/recipient knows. SS is very difficult to crack because of how the private key is generated. Finding the factorization of primes is known to be especially difficult. So we obtain two very large primes p and q and the public key is given as

$$n = p^2 q$$

where n is the public key. We can then determine the private key as

$$d = n \mod \lambda(pq)$$

where $\lambda(pq)$ is given by

$$\lambda(pq) = \mathrm{lcm}(p-1, q-1) = \frac{|p-1||q-1|}{\gcd(p-1, q-1)}$$

Then given a message M we can encrypt it using

$$E(M) = c = M^n \mod n$$

Conversely, to decrypt the cipher text, c, we use the private key,

$$D(c) = M = c^d \mod pq$$

To have effective encryption, we need our public and private keys to be sufficiently large and this means using more than 64 bits, which is the maximum the standard `C` provides. Thus I learned to utilize the GNU Multiple Precision, `gmp`, library, which emulates numbers far greater than 64 bits can.

Additionally, in order to write the message or cipher text to a file we needed to split it up into blocks and write each block in a buffer.

2 What I Learned

In this assignment, I learned to use a buffer. I didn't really understand what a buffer meant in the context of programming until now, actually implementing it. I think it was helpful to already have done some cryptography in my CSE30 Python class but I now understand a lot of the abstraction used from those assignments.

I also learned to use a significant portion of the `gmp` library. This includes setting, comparing, and altering variables as well as importing and exporting arrays to and from `gmp`.

Additionally, I now understand how to *declare*, *define*, and use global variables with `extern`. This was vital to use the same `state` for all calls of `gmp` random functions.

On the line of debugging, I learned to use `gdb` to diagnose some segmentation faults and I also found a lot of use in `valgrind` with the `-g` flag to find memory leaks and errors.

3 Cryptography in the World

Public-private key cryptography is used abundantly in the world. More popular than SS, RSA (Rivest–Shamir–Adleman), while aging, is used in many applications such as web browsers, VPNs, and communication channels. (Lake, 2021) Pretty much everything sensitive has some sort of encryption, and asymmetric cryptography (specifically RSA or SS in our case) is very effective to accomplish the desired security.

A specific instance, for me personally, is creating SSH keys that use RSA to generate public and private keys. This can then be used to establish a secure connection to GitHub. I use this functionality daily for this class and in general when I work on my programming projects.

4 Conclusion

Overall, I learned a lot about the details of public-private key cryptography as well as the `gmp` library, which makes me more confident to learn complicated libraries in the future. I also understand the importance behind cryptography since it's used to keep everything on the internet and sensitive information secure.