# WRITEUP

KirkAngelo Perez *

February 26 2023

This was a difficult assignment to do. The math was hard and we also had to learn about GMP. It's to be expected since we're implementing cryptography. It was a great learning experience. This was also extra interesting since we're applying concepts that have completely shifted the way the world works. Public-private cryptography has a wide range of uses; from encrypting, authenticating, verifying, key generation, and much more. Personally, I use a lot of websites that rely on Cloudflare. They're all about cryptography and they provide an essential service to the Internet's safety and ability to operate the way we know it. What public-private cryptography essentially does is allow for a safe way for people and computers to exchange information to only their intended targets.

## 1 ss.c

This was where most of our code was located. Most of the new concepts from the assignment were focused around here too. We're now making use of mpz_t too. Data of those types have to be handled differently. We can't simply just conjure them up and give them arbitrary values easily as we do with normal variables. First, we declare like normal. Then, if you want to do a function, you'll have you to use an mpz specific function. For example, if you want to set an mpz value, you'll have to use mpz_set(). A large part of the difficulty of the assignment was having to search through the documentation, but I learned a ton by having to do that.

## 2 numtheory.c

This file was very math-heavy and also took a while. In a way, a lot of it was straightforward as the pseudocode was provided, but again, having to use GMP functions made it difficult. The two main ones that caused trouble were is_prime and mod_inverse.

## 3 keygen.c and randstate.c

These are also straightforward files. In randstate.c, make sure to declare state. We have it declared in our .h file, but we need it in our .c in order to actually define it. Keygen was simple and you really just had to follow the order given in the assignment pdf. An interesting code snippet was the fchmod() and fileno() part. I didn't initially know how to use it, but it wasn't hard to understand once I finally got it typed out.

## 4 decrypt and encrypt

These two files are very similar. They're almost the exact same; just have slightly different variables and call the opposite version of what you have (priv to pub or pub to priv). In each of them, I declared the respective variables and made nearly identical switch statements. The actual "body" or "content" code-wise in these files consisted of opening a file, reading it, encrypting/decrypting it, and then closing the file. Not too hard.

*1918126