Assignment 5
WRITEUP
Prof Veenstra
Nguyen Vu

In this assignment, I implement the Schmidt-Samoa (SS) Algorithm for encryption and decryption data in C programming language and in this WRITEUP.pdf, I will talk about everything I learned while doing this assignment.

1. General knowledge gain

1. I learn and use the GMP library and mpz variables for the first time and learn that they are precise integers that have memory dynamically allocated and reallocated.
2. These functions I had a lot of trouble with that are also in the GMP library so I will put them in a new section. They are mpz_export and mpz_import. These functions have multiple parameters that I didn't really understand, but the TAs really helped me breaking down the function so it's easier to understand.
3. I learn how to implement more complex number theory equations in code such as greatest common divisor, modulo inverse, exponential modulo, and check whether a number is prime or not using Miller-Rabin method.

2. My understanding of cryptography

Before this assignment, I thought cryptography is just having a data and change it in a specific rule and the receiver simply reverse the rule. Now, I learned that my initial thought was somewhat correct, but to create the rules so that it's difficult to break for the non-receiver is a process that takes a while to complete. I also learned that the 'rules' don't need to be concrete as the keygen.c makes a new 'rule' every time we use it.

3. How does cryptography affect the world at large?

During World War 2, the Enigma machine made by Germany used encryption to transfer messages to their side without the Allies knowing what are they saying. England eventually created a machine that can decrypt what the Enigma encrypted and that was a major step in helping the Allies winning the war at the end. Cryptography was used in a war that without the decryption, it would cost more lives and time to end it. In today's world, cryptography is used in various things especially when it comes to the internet. Online shopping, bank transaction, email, etc. cryptography is working in the background to make sure your data is safe.

4. How do you utilize this type of cryptography as part of your

daily life?

I don't think there is anything that I need to make an encryption on my own for now, however, I still use a lot of built in cryptography system on the internet, One of the most common one is through the use of secure communication channels, such as encrypted messaging apps or email services that use encryption protocols to protect my messages from being intercepted or read by unauthorized parties. Additionally, I may use cryptography when making online purchases or accessing secure websites that require me to enter sensitive information, such as credit card details or login credentials.