Can you (De)Crypt it?

Mylo Lynch

February, 28, 2023

1 Intro

Why am I the only one who can access my private messages? Why can I trust online services to not peer into all of my deepest, darkest secrets? How can I communicate with someone privately without them being in my vicinity? These are questions the general population won't even bother to even ask or worry about since encryption has become so essential. Encryption has become a mainstay in our day to day lives, yet most people are not even aware of such a fact! But how does it even work?

In this assignment, we have to understand and implement Schmidt-Samoa public/private key encryption. A decent proficiency with number theory, as well as GMP is required for this assignment.

2 Key Takeaways

First things first, I had to learn how to use the GMP library for this assignment. It was a whole lot of reading, and a whole lot of rereading, but now I am able to manipulate data from bits, to hexstrings, back to bits, and into characters and integers! Being able to use such a tool is going to be essential once we go off into the industry and work on much larger projects. ESPECIALLY if one is to go into encryption specifically (as many companies won't do their own encryption).

Second, a good understanding of number theory (especially anything having to do with modulus) is necessary in order to implement the logic behind the even making the keys, let alone using them to encrypt and decrypt messages! I had never encountered the idea of a modular inverse or modular exponentiation(though I soon learned how useful the modulus operator is in coding thanks to the property the n % m can only equal to a value between 0 and m-1). However, I had enough familiarity with finding the greatest common divisor of two numbers, as well as finding their lowest common multiple that I could focus the majority of my reading time learning how to use the gmp library and trying to understand the modular parts of number theory. By taking coprime prime numbers, you can multiply one by the square of the other and get rid of the original values in order to create a key that should be near impossible to crack! Using what we learned with modular exponentiation, inverses, gcd, and lcm, we can then encrypt the data we manipulated into an unrecognizable encryption. This is especially essential to online messaging apps.

3 Conclusion

How do I plan on taking advantage of encryption in my day to day life? By being as cheesy and loving to my partner and calling her the goofiest, dumbest, most absurd names on the planet every single day... MULTIPLE times a day, without fear of someone being able to read what I'm sending and turning me into a meme somewhere on some sort of social media. My stupid nicknames will remain safe until the end of time (unless screenshots get out).