WRITEUP

Wenyu Liang

February 27, 2023

1 Program description

There are three programs for this assignment. They are keygen, encrypt and decrypt. The keygen program will be in charge of key generation, producing SS public and private key pairs. The encrypt program will encrypt files using a public key, and the decrypt program will decrypt the encrypted files using the corresponding private key.

2 What I learned

1. **gmp library:** I learned how to use gmp library from this assignment and chances are I will use it in the future since it's a very useful package for arbitrary precision arithmetic
2. **SS algorithm:** I know how each part of the algorithm works now
3. **numtheory functions:** I learned a lot of numtheory functions and am able to implement them. I also leaned the algorithm to test if a number if a prime.

3 How my understanding of cryptography changed

I didn't what private key do when I first used ssh public key because I didn't use the private key at all, but now I know private key is required when you want to decrypt an encrypted message. I thought cryptography was just using very large random number and keep it from people who we don't want them to know, but now I know cryptography relies on the assumed difficulty of factoring large composite integers.

4 How does cryptography affect the world at large

In general, encoding and decoding messages to keep them secure from unauthorized access. In details, here are some aspects that are influenced by cryptography:

1. **Secure communication**:secure communication between individuals, organizations, and governments
2. **Online transactions**: secure online transactions such as online shopping, banking, and other financial transactions.
3. **Data protection**: protect data in transmission

5 How I utilize cryptography in real life

When I send message to my friend, I can encrypt my messages and only my friend can see it when I give them the private key. We can also use VPNs to encrypt our internet traffic and protect our online activities