Nicolas Corfmat
CSE13S, Winter 2023
ncorfmat@ucsc.edu

Cryptography:
The Backbone of Cybersecurity

Assignment 5: Public Key Cryptography

1 Description of Program

This program uses public-private key cryptography to encrypt a user-specified message using the generated public key, and then decrypting it using the corresponding private key. There are three main programs: *keygen*, *encrypt*, and *decrypt*. The *keygen* program generates SS public-private key pairs which are then used by *encrypt* and *decrypt*. The public key is used by *encrypt* to securely encrypt files, while *decrypt* makes use of the private key to unlock, or decrypt, files.

2 The Necessity for Encryption

In the digital age, information is constantly being sent and received, and sometimes this data can contain confidential material. Imagine a world without encryption, therefore making all information public and accessible by anyone. Governments would exploit this by stealing sensitive documents from each other, thieves could effortlessly tap into bank accounts, and privacy would overall cease to exist—this world illustrates a hacker's fantasy.

Fortunately, there exists the ability to envelope private information so that you can specify who gets to view it, and that is with the help of *encryption*. Some advantages of encrypting data include confidentiality, the ability to detect alterations to private information, ensure a message came from the listed sender(s) and were received by said recipient(s), and the guarantee that the encrypted message was transmitted by the authenticated sender.

It is important to remember, encryption does not guarantee all of this. There always remains the possibility of a code-break or someone maliciously gaining access to confidential material. However, this approach significantly reduces the risk of unwanted parties accessing restricted information by means of discreteness and concealment.

3 The Program

The program makes use of a certain kind of encryption—*public-private key encryption*. Essentially, the code generates a matched pair of keys, saving the private key to yourself and providing you with a shareable public key. These keys are comprised of large, unique numbers, so that they become exceptionally tougher to crack using means such as brute-force. In the C language, the range of *int*'s, *long*'s and *long long*'s are not sufficient to reach the level of security we are aiming for. As a result, we make use of the GNU Multiple Precision Arithmetic Library to work with large numbers that would have otherwise been impossible with the data types available in C.

Additionally, the importance of prime numbers repeatedly surfaced throughout this assignment. The reason encryption algorithms opt for prime numbers instead of standard non-prime values is to make it impossible to factor out these large numbers. Suppose a computer were to brute-force the factors of a large number; in that case, our generated public and private keys become easily decipherable. Working with prime numbers greatly reduces the program's susceptibility to cracking algorithms.

Lastly, unlike traditional C data types, multiple-precision integers do not free themselves—they will continue taking up space in the stack until they are de-allocated from memory. The reason we need to ensure every "mpz_t" object is released after it has been used is to prevent potential memory leaks. In order to optimize the limited memory in our system, we must confirm that all created objects have been de-allocated.

4 Applications of Public-Private Key Cryptography

It is fair to say the importance of encryption has been established by this point; it ensures information remains private between parties. In the modern world, this form of cryptography is used for reasons such as securely processing online transactions, safely logging on to personal accounts, and exchanging digital messages to name a few.

In my own experience, I personally benefit from public-private key encryption whenever I communicate with friends online. Primarily on the social desktop app, Discord, it provides me with a level of reassurance knowing that my conversations are not being read by unwanted guests (remember, not a guarantee). Thanks to cryptography, gossip remains undisclosed.

5 Conclusion

Ultimately, the concept of cryptography is essential to protecting private information across virtual channels. Not only does it ensure confidentiality, it also mostly guarantees sender authenticity and reveals any alterations to a message. While almost all forms of encryption carry the risk of being cracked, this task is extremely difficult and computationally intensive for most modern computers. Our implementation of public-private key encryption makes use of mathematical conversions and randomness to generate key pairs, ensuring information is securely encrypted and decrypted. Today, cryptography is becoming an ever so important component of cybersecurity, as highly sophisticated AI pose a threat to virtual integrity.