Assignment 5 Writeup: Cracking the Secrets to Data

Sep Nasiriany

Due Date: February 26, 2023

1 Introduction

The modern world revolves around data, especially now that we're deep in the 21st century. Banking, healthcare, commerce, and almost everything that we depend on today depends on the security of data. If this security is compromised, it poses a great threat to activities we mindlessly do each and every day. Even before the advent of the internet and modern computers, encryption was essential for centuries in order to secretly and securely relay a message to the intended recipient. Encryption comes in 2 conventional forms: asymmetric and symmetric encryption. Symmetric encryption has the flaw of using the same key to encrypt and decrypt a message. Asymmetric encryption, on the other hand, involves using the public key of the recipient to encrypt a message and a private key that only the recipient knows to unlock that messages. When this is used with a well known and secure algorithm like RSA, it creates a virtually uncrackable message that only the recipient can unlock. This assignment used the asymmetric Schmidt-Samoa algorithm, similar to RSA, in order to encrypt and decrypt messages. Figure 1 explains this phenomenon well.

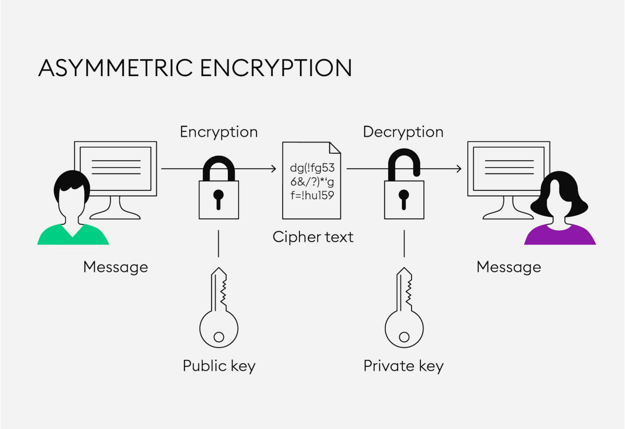


Figure 1
Diagram explaining Public-Private Key Encryption. Only Person A can receive the message from Person B because their private key is not known to outsiders. Image from
`https://www.bitpanda.com/academy/en/lessons/what-is-asymmetric-encryption/`

2 SS Encryption - Lessons Learned

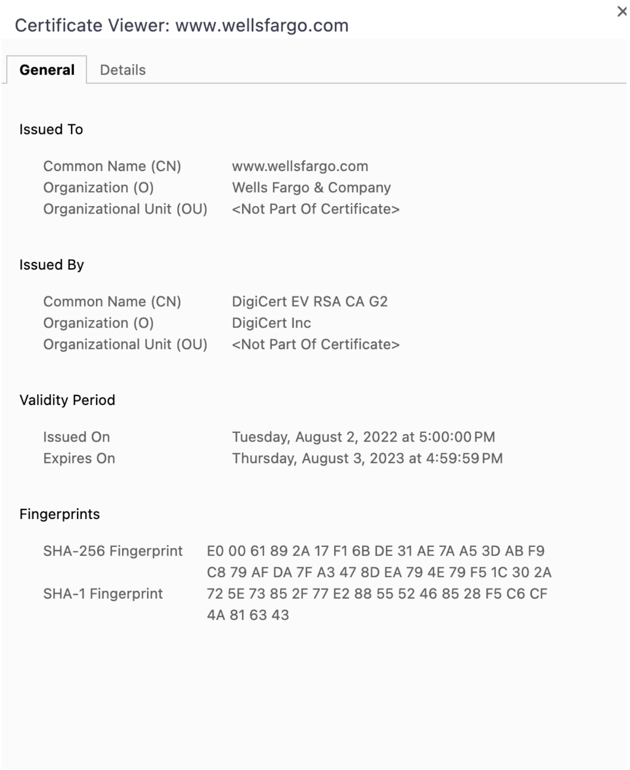
The Schmidt-Samoa (SS) algorithm taught me a lot about what's going on under the hood with regards to encryption. I was quite confused about how exactly asymmetric cryptography worked until I actually had to implement it myself. For starters, SS produces a `n` value of 2 prime numbers `p` and `q`. Now, `n` is actually equal to p^2q. Why does it have to be prime? Because prime numbers don't have any factors, it's very hard to factor the product of 2 prime numbers, while it's very easy to multiply them. If we know the numbers that contributed to making n and our enemy does not, we can use those factors p and q to decipher what was being said using modular exponentiation.

So going back to lessons learned, I learned exactly all the math that goes behind making encryption work. Almost everything related to the SS algorithm comes down to modular arithmetic and Euler's theorems. I learned a lot about the `gmp.h` library and why it was being used. Native C integers could not possibly handle the handling of such massive numbers, and the security of SS is reliant on producing 2 prime numbers that are sufficiently large enough that they cannot be discovered by brute force. I learned that the `gmp.h` operates on memory allocated to the heap and has to have its memory freed and cleared, which is why we had to use `mpz_clear()`. I learned quite a bit about file I/O and this was the first assignment I was able to use functions like `getenv()`, `fchmod()`, and `fileno()`. Granting file permissions was something I never knew about either, but it's absolutely crucial in order to prevent another user from snooping on the private key used to decrypt files. Finally, I learned how to make 3 executable files in such a way that doesn't utilize a C file with another `main()` function.

3 How Cryptography is Used Everyday

So how is encryption used in our lives? It's happening almost all the time when your visiting a website. In fact, there is a way for you to see exactly how each website in encrypted, when you click the lock button on the left of the URL on your browser. Below is a figure of the encryption certificate used at Wells Fargo's website, which is very crucial for keeping banking secure. Very secure encryption is so widespread that it's almost a better question asking where encryption is not being used. Encryption, as it turns out, is also sometimes the mandated law for companies to use. The Health Insurance Portability and Accountability Act (HIPAA) requires that patients' data be encrypted using AES and this ensures that the privacy and confidentiality is protected. Much of social media and messaging apps are encrypted. One reason why the Signal App is popular is because it is well known for its end-to-end encryption. Apple's iMessages also features end-to-end encryption which means that in theory Apple cannot access messages sent between multiple users. Only the sender and recipient can access the contents of the messages sent between one another.

Another reason we might have encryption is so that other big name entities like the federal government cannot spy on us and surveil citizens. This has, however, become a rambunctious issue because governments mandate that companies like Facebook must hand over encrypted data when necessary in order to investigate criminal activity. Criminals themselves abuse this vital protection and that has sparked a debate about how much encryption is necessary. At the same time, encryption is very vital in national security, considering the constant threat that adversarial countries are always making attempts to hack sensitive information.



Certificate Viewer: www.wellsfargo.com

Issued To

Common Name (CN)	www.wellsfargo.com
Organization (O)	Wells Fargo & Company
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	DigiCert EV RSA CA G2
Organization (O)	DigiCert Inc
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Tuesday, August 2, 2022 at 5:00:00 PM
Expires On	Thursday, August 3, 2023 at 4:59:59 PM

Fingerprints

SHA-256 Fingerprint	E0 00 61 89 2A 17 F1 6B DE 31 AE 7A A5 3D AB F9 C8 79 AF DA 7F A3 47 8D EA 79 4E 79 F5 1C 30 2A
SHA-1 Fingerprint	72 5E 73 85 2F 77 E2 88 55 52 46 85 28 F5 C6 CF 4A 81 63 43

Figure 2
Encryption certificate used for Wells Fargo’s website. It uses SHA encryption (hash encryption) which is considered to be asymmetric.

3.1 How I personally utilize Encryption:

I personally have started using the Signal app for over a couple years because it’s very well known for its end-to-end encryption abilities. Credit card readers that scan my credit are encrypted so that credit card information cannot be accessed from the outside. Emails that are sent and received daily through my ucsc.edu account are all encrypted using TLS (Transport Layer Security). HTTPS (Hypertext Transfer Protocol Secure) itself uses encryption so that sensitive information is protected. I also use Google Photos and Google Drive, and they use encryption for anything that's stored into their servers to protect the content of their users. Again, it's pretty hard to find what's not being encrypted in today's day and age of constant communication over the web.

4 Citations

I would like to acknowledge Professor Long for the pseudo code provided in the assignment doc because that helped me a lot with `numtheory.c`.