Cryptography Library Research Paper

Long Pham

Shiley-Marcos School of Engineering (SMSE), University of San Diego

CYBR-592-01B: New Student Orientation

Professor Haydar Majeed

April 27, 2025

Cryptography is an important area in cybersecurity that deals with securing and hiding data using various algorithms and techniques such as cryptographic keys and encryption. It is an area that I have some experience with as I took a class recently that covered cryptography. I learned many important topics in this class such as symmetric and asymmetric keys, encryption, and hash functions. I also applied my knowledge and developed my skills by completing the various assignments in this class. These assignments made me utilize various cryptographic tools and algorithms such as OpenSSL, SHA256, and Steghide.

As a result of my previous experience with cryptography, I have become interested in the more complex topics surrounding cryptography. Considering my previous experience with hash functions, I wanted to learn more about them. This led me to an interesting article that discusses pseudorandom numbers and hash functions from iterations of multivariate polynomials. In this article, Alina Ostafe and Igor E. Shparlinski "propose a new construction of hash functions based on iterations of polynomial systems" (Ostafe & Shparlinski, 2010, p. 64). This new construction involves multiple steps. One such step involves choosing an initial vector $\mathbf{w_0}$ (Ostafe & Shparlinski, 2010). Another step involves applying the polynomial systems iteratively starting at $\mathbf{w_0}$ to obtain a sequence of vectors $\mathbf{w_j}$ (Ostafe & Shparlinski, 2010). All of these steps lead to the output $\mathbf{w_J}$ which is the value of the hash function and can be interpreted as a binary $(m + 1)n$-bit string (Ostafe & Shparlinski, 2010). This article furthered my understanding of hash functions and taught me a new way to utilize hash functions. The information outlined in this article will help to further secure hash functions and make them harder to break.

In addition to hash functions, I wanted to learn more about encryption considering my previous experience with the topic. This led me to an interesting article that discusses doing an affine cipher encryption using a residue number system. In this article, the authors outline a new

efficient technique to encrypt information flows based on a combination of affine ciphers and the residue number system (RNS) (Kasianchuk et al., 2025). This combination of affine ciphers and the RNS "provides an additional level of protection by dividing the numeric notation of characters into several independent components" (Kasianchuk et al., 2025). This combination eliminates the vulnerabilities of affine ciphers by using the advantages of the RNS (Kasianchuk et al., 2025). This combination also complicates cryptanalysis by forcing the attacker to "take into account the number of moduli and their combinations" (Kasianchuk et al., 2025). This article furthered my understanding of ciphers and encryption as well as taught me new ways to utilize ciphers and encryption. The information outlined in this article will help lead to the development of stronger encryption methods.

Although I have some knowledge of cryptography, there is still a lot that I can learn when it comes to this area. There are many articles that have been published discussing complex issues surrounding cryptography. These articles provide unique perspectives on certain topics in cryptography such as hash functions and encryption. They also offer new solutions to address the complex issues surrounding cryptography. In the end, all of these articles will help contribute to the advancement of cryptography.

References

Kasianchuk, M., Shevchuk, R., Adamyk, B., Benson, V., Shylinska, I., & Holembiovskyi, M. (2025). Affine Cipher Encryption Technique Using Residue Number System. *Cryptography*, *9*(2), 26. https://doi.org/10.3390/cryptography9020026

Ostafe, A., & Shparlinski, I. E. (2010). Pseudorandom numbers and hash functions from iterations of multivariate polynomials. *Cryptography and Communications*, *2*, 49–67. https://link-springer-com.sandiego.idm.oclc.org/article/10.1007/s12095-009-0016-0#Equ1