Cryptography Implementation of One or Many

The focus behind this paper is cryptography and whether it is best to use a single method or a combination of different ones. There are many ways to encrypt your data. The method we know best is the asymmetric and symmetric ciphers created by using public and private keys. The keys are ones that we see a lot, but it is best used with watermarking. The keys are useful by themselves, but they have trouble with needing to communicate the key ahead of time and sending the key could lead to it being known by outside people. Watermarking is a useful way of making sure that the person sending or receiving the data is indeed the intended person. Baldimtsi and the others who wrote the watermarking article give a great example on watermarking with a VPN customer, “*Watermarking a VPN client could potentially restrict an employee from sharing its client*” ( Baldimtsi). In his example, each employee has their own private and public key so with the watermark, the client will be working with that single employee. Watermarking is used with the keys so while it is an additional safety measure, it is reliant on others.

Another cryptography implementation is brought in by Dexi Wang and their group about hashing. Hashing can take a lot of forms but at its base, it is an algorithm that maps data to a fixed length. Wang best sums up hashing as follows; “*A cryptographic hash function protocol is usually designed to ensure the correctness of its hash algorithms,”* (Wang). Comparing the keys and hashing shows that while they fall under cryptography, they both have different roles to play as one will encrypt, the other will validate.

Pal wrote an article about artificial neural networks and their use in cryptography. Pal uses the asymmetric and symmetric encryption methods and creates the key using a generation algorithm called tree parity machines, which will take user input, change it into ASCII, split it in two, run through an equation then compared. If the two parts come out the same, then it will run further through the algorithm. The algorithm is used to generate different cipher text each time so the same input will have different padding. “*Due to this dynamism it is almost impossible for the intruder to detect the actual information even the information is passing through an insecure public channel*” (Pal).

Looking into cryptography shows that each method can be built off and can become more secure with these addons. Putting the methods together we have watermarking, hashing, and asymmetric/symmetric encryption with secret keys. Nazaruk and Rusakov explain what exactly cryptography is, “*Cryptography is a science which investigates methods of protecting information. Protection of information is an activity (or a set of activities) for providing security of the information*” (Nazaruk & Rusakov). They further go on to mention the three main parts in information security which is confidentiality, integrity, and authenticity. These sections together are also known as the CIA triad in cryptography. By themselves, the methods we discussed can each cover one of the three parts. Together, the three sections are more secure than individually.

Watermarking is a way of giving a signature on the encrypted data. This can be used for the authenticity part of the triad leaving the other two open. Adding on the hashing, we cover the integrity of the data as it can make sure there have not been any changes. The confidentiality comes in the form of the asymmetric/symmetric keys and how they are used to encrypt data. Each part has a point in the process that they can cover so that security is in play every step of the way. Starting with key creation which we can use Pal’s algorithm for, then encrypting the messaging giving it a watermark. Sending it to the person who can make sure there has not been any changes on its way over with hashing and making sure the watermark is there for authenticity. While having one part will increase security, by using different methods, we are able to cover more sections of cryptography and make the process more secure.

References

*Baldimtsi, F., Kiayias, A., & Samari, K. (2021). Watermarking public‐key cryptographic functionalities and implementations: The case of encryption and signatures. IET Information Security (Wiley-Blackwell), 15(3), 205–222.* [*https://doi-org.links.franklin.edu/10.1049/ise2.12013*](https://doi-org.links.franklin.edu/10.1049/ise2.12013)

*Dexi Wang, Yu Jiang, Houbing Song, Fei He, Ming Gu, & Jiaguang Sun. (2017). Verification of Implementations of Cryptographic Hash Functions. IEEE Access, 5, 7816–7825.* [*https://doi-org.links.franklin.edu/10.1109/ACCESS.2017.2697918*](https://doi-org.links.franklin.edu/10.1109/ACCESS.2017.2697918)

*Nazaruk, V., & Rusakov, P. (2010). Implementation of Cryptographic Algorithms in Software: An Analysis of the Effectiveness. Computer Science (1407-7493), 43, 97–105.*

*Pal, S. K., Datta, B., & Karmakar, A. (2022). An Artificial Neural Network Technique of Modern Cryptography. Journal of Scientific Research, 14(2), 471–481.* [*https://doi-org.links.franklin.edu/10.3329/jsr.v14i2.55669*](https://doi-org.links.franklin.edu/10.3329/jsr.v14i2.55669)