Article Citation Format
Abanga, E.A. (2022): Symmetric, Asymmetric and Hash Functions.
Journal of Digital Innovations & Contemporary Research in Science,
Engineering & Technology.
Vol. 10, No. 2. Pp 55-60
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P7

Symmetric, Asymmetric and Hash Functions

Abanga Ellen Akongwin
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: ellen.abaga@st.gimpa.edu.gh
Phone: +233540337659

ABSTRACT

The field of cryptography offers numerous methods for transmitting data securely through networks. It usually builds and evaluates several protocols that deal with the numerous facets of information security, such as confidentiality, integrity, etc. Modern cryptography includes a number of engineering and scientific areas. Everyday uses of cryptography include things like computer passwords, ATM cards, and electronic commerce. The term "cryptography" refers to a method of protecting data from unauthorized parties by converting readable and stable information into an unknowable form that can be deciphered on the other end to obtain the needed information using the decoding method supplied by the message's creator.

Keywords: Hash function, encryption, symmetric key, and cryptography

1. INTRODUCTION

Cryptography is a method of limiting the transmission of undisclosed messages. Greek speakers use the term to refer to "secret communication." However, at the moment, cryptography successfully provides the privacy of people and organisations, ensuring that the details of data conveyed are encrypted in a manner that only the receiver may retrieve the details of data (Verma et al., 2021). Despite the fact that the majority of users are unaware of it while using it, many individuals and organisations use cryptography every day to safeguard data and its specifics around the world. It is also seen as being overused and extremely delicate since cryptography devices can be compromised by a single code or instruction error (Verma et al., 2021). In order to prevent any unauthorized access to information that is stored on storage devices or traveling across communication channels, classification cryptography is used to jumble the data. Additionally, cryptography is used to confirm the method by which separate parties attempt to use the system in any way.

Since a group must produce evidence that they are indeed who they claim to be in order to be granted a specific benefit under the system (Chauhan & Khetan, 2019). That something is occasionally referred to as certifications, and further precautions must be made to ensure that these certifications are only used by their rightful owner. The greatest and most obvious credentials serve as passwords. Username and password are encoded to prevent unauthorized use. Confirmation is a layer based on approval since the gathering is validated by demonstrating the necessary qualifications (passwords, keen cards and so forth) (Chauhan & Khetan, 2019).

Following the acceptance of the qualifications, the authorization procedure is initiated to ensure that the mentioned party has the assent to do the capacity required. Techniques for computerized signature, a process that includes executing cryptography among other things, are used to achieve information respectability and non-repudiation. In this paper, we will look at various cryptographic encryption approaches (Chauhan & Khetan, 2019).

2. RELATED LITERATURE

According to Lincke and Holland (2007), teaching computer security is like aiming at a shifting target since computer and network security is a new and developing field of computer science. The main focus of security courses is on algorithmic and mathematical ideas, like encryption and hashing techniques. As crackers find new ways to breach network systems, new courses are designed to combat these attacks; nevertheless, as a result of the responses from new security software, each of these attacks quickly becomes outdated. With the ongoing development of security language, business practice, network management, infrastructure security, and legal foundation all continue to benefit from the emergence of security approaches and skills.

Abomhara et al. (2009) presented the fundamental concepts, features, and aims of cryptography. They talked about how communication has helped to advance technology in our time, the information age, and how it is crucial to protect privacy when data is transmitted via communication. Data security is given top attention when utilizing encryption techniques to ensure that data reaches the end user safely and without being compromised, according to Al Busafi and Kumar (2020). Data communication is described as relying mostly on digital data transfer. They also illustrated the various symmetric and asymmetric cryptography algorithms that are employed in the transmission of data.

According to Lee and Jang (2020) a network encryption and security study, organisations all over the world generate massive amounts of data on a daily basis as a result of the expansion of social networking websites and commerce applications. As a result, information security has become a major problem in terms of maintaining the protection of data transit across the internet. This issue illustrates the growing importance of cryptographic approaches as even more individuals access the internet. This paper provides an overview of the many security-enhancing approaches used by networks, including cryptography. Al-Shabi (2019) discussed the background and importance of cryptography, and also why information security has developed into a challenging problem in the fields of information and communication technologies. This paper provides various asymmetric algorithms that already have given us the ability to safeguard and secure data, in while also demonstrating cryptographic techniques as a method for ensuring identifying, accessibility, honesty, and by offering security and privacy, users' and their data's privacy.

Singh and Singh (2019) did a study on encryption, privacy enhancing technologies, legislative developments related to cryptography, reliability, and privacy enhancement technologies. He stated that how civilization uses cryptography will decide its future, which is determined by regulations, present laws, and practices, in addition to what society wants it to achieve. He claimed that there are many gaps in the field of cryptography that need be filled by future researchers. The advancement of cryptography also requires a management system that creates strong keys to ensure that only the right people with the right keys may enter and others who lack the keys cannot.

Dhanaji et al. (2000) came to the conclusion that security secrecy is not a good thing and that it is bad for protection to be hidden because security that only depends on secrecy can be weak. It would be difficult to regain that secret if it was lost. Schneier went on to say that in order to provide effective security, cryptography based on brief secret keys that are simple to transfer and alter must adhere to a fundamental concept, according to which the cryptographic algorithms must be both powerful and well known. Accepting public inspection is the only surefire approach to achieve further improvements in insecurity.

Sultan et al. (2020) stated that many conversations and advancements are created about cryptographic techniques, According to the author, hash functions are crucial to cryptography because they can assign almost any value to any set of data, and as time went on and MD5's faults were made public, it created uncertainty about how to construct hash functions. Sadkhan and Mohammed (2015) highlighted the primary processes and trends of the fields of cryptography from Julius Caesar to the modern era, as well as the state of the Arabic industrial and scholarly efforts in this field in the past era that are connected to the clearly established cryptographic techniques and search for new evaluation techniques for information security.

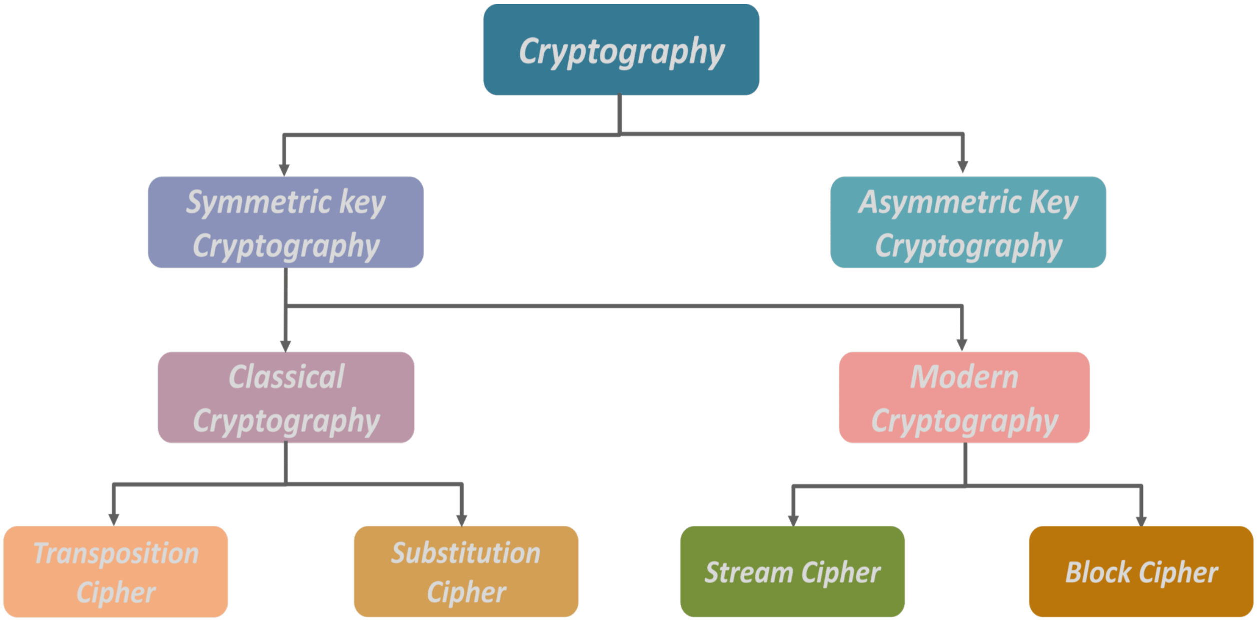

Figure 1: Cryptography concept

2.1 Symmetric Encryption Methods:

With symmetric-key encryption, it is possible to deduce the encryption key from the decryption key and vice versa. The use of symmetric keys can be extremely efficient, ensuring that clients do not experience any significant time delays as a result of encryption and decryption. Symmetric-key encryption also adds a level of security because data encoded with one symmetric cryptography cannot be decrypted with another symmetric key. As a result, as long as the symmetric key is kept silent by the two parties using it to encrypt conversations, each party can be certain that it is conversing with the other as long as the decoded messages appear normal.

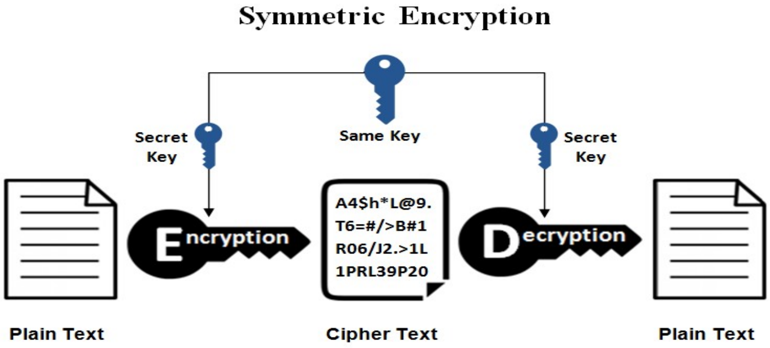

Figure 2: Method for Encrypting General Symmetric Keys
Source: SSL2BUY Wiki

2.2 Encryption with Asymmetric Keys

The most widely used asymmetric-key (Chauhan & Khetan, 2019) encryption solutions are built using RSA Data Security's patented techniques. The RSA method of public-key encryption is therefore discussed in this section. A pair of keys, a public key and a private key, are used in asymmetric key encryption (also known as public key encryption), which is used to secure and authenticate data. Due to the fact that each public key is made public and the corresponding private key is kept secret, data encrypted with one key can only be decoded using another key. According to the diagram in Figure 2, a distributed public key is used for encryption. Generally speaking, in order to communicate encrypted data, one must first encrypt the data using the recipient's public key.

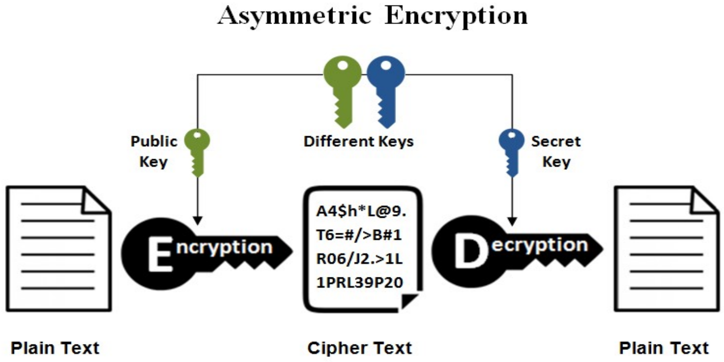

Figure 3: Method for Encrypting General Asymmetric Keys
Source: SSL2BUY Wiki

2.3 The Hash Function

No key is used by hash functions, which are also known as message digests. Instead, a fixed-length hash value based on the plaintext is created, making it impossible to reconstruct the plaintext's length or contents. The secrecy and integrity principles are mostly attained using hash methods. When we don't trust the individual with whom we are exchanging information, hashing methods come in handy. Send the other party the list of digests if, for example, you have a suppression list of email addresses and you want them to be deleted from their database but you don't want to actually share the list of email addresses with them. Through their database, they may produce the digest for each of the email addresses of them.

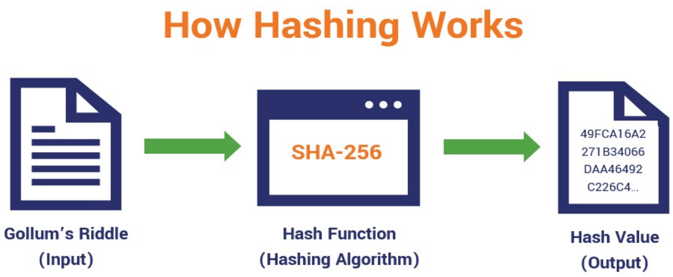

Figure 4: Method for hashing
Source: SSL2BUY Wiki

3. RESEARCH GAP

Future researchers should close many gaps in the field of cryptography. Furthermore, a management solution that creates strong keys is essential for the continued success of cryptography since it will guarantee that only authorised users with the right keys can access data and that unauthorised users cannot (Al-Shabi, 2019). Additionally, the literature search on symmetric, asymmetric, and hash functions that was done using databases including E-Journals, Google Scholar, Education Science, Research Gate, Emerald, and Academic Journals provided scant results with minimal literature in sub-Saharan Africa, particularly Ghana. This illustrates the urgent need for study on symmetric, asymmetric, and hash functions in understudied countries like Ghana. In light of all of this, the primary objective of this study is to add to the body of knowledge on symmetric, asymmetric, and hash functions in developing-country higher education institutions by elucidating their significance and advantages.

4. FINDINGS

Chauhan and Khetan (2019) established that cybersecurity education is an ever-moving target and that computer and network security is a brand-new, rapidly-evolving technology within the computer science field Security courses place a strong emphasis on algorithmic and mathematical principles such as hashing algorithms and encryption. The management system that creates stronger keys is essential to the future of cryptography since it will ensure that only authorised users with the correct keys can access data and that unauthorised users cannot (Callas, 2007). Chachapara et al. (2013) discovered that users of the cloud can generate keys for numerous individuals with various levels of access to their content.

5. CONCLUSION

Cryptography is essential in fulfilling the primary goals of security, such as authentication, integrity, confidentiality, and no-repudiation. To fulfill these objectives, cryptographic algorithms are created. Cryptography serves a crucial purpose by ensuring the security of networks and dataIn this article, we summarised some of the research that has been done on the topic of cryptography and demonstrated the operation of the many cryptographic techniques used for varied security needs. In order to safeguard personal, financial, medical, and e-commerce data while still providing a decent amount of privacy, cryptography will continue to advance in IT and business planning.

REFERENCES

Abomhara, M., Zakaria, O., & Khalifa, O. O. (2009). An Overview of Video Encryption Techniques. *International Journal of Computer Theory and Engineering*, 103–110. https://doi.org/10.7763/ijcte.2010.v2.123

Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), p8779. https://doi.org/10.29322/ijsrp.9.03.2019.p8779

Al Busafi, S., & Kumar, B. (2020). Review and analysis of cryptography techniques. *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*, 323–327. https://doi.org/10.1109/SMART50582.2020.9336792

Chauhan, J. S., & Khetan, N. (2019). *A Review Paper on Symmetric Key , Asymmetric key Encryption and Hash Function*. 193–195.

Dhanaji, A. S., Gajanan, K. P., & Pandurang, K. A. (2000). *A Research Paper on Cryptography*. *3307*, 328–336.

Lee, M. S., & Jang, D. J. (2020). A survey of blockchain security issues. *JP Journal of Heat and Mass Transfer*, *2020*(Special Issue 1), 29–35. https://doi.org/10.17654/HMSI120029

Lincke, S. J., & Holland, A. (2007). Network security: Focus on security, skills, and stability. *Proceedings - Frontiers in Education Conference, FIE*, 10–15. https://doi.org/10.1109/FIE.2007.4417898

Sadkhan, S. B., & Mohammed, R. S. (2015). Proposed Random Unified Chaotic Map as PRBG for Voice Encryption in Wireless Communication. *Procedia Computer Science*, *65*(Iccmit), 314–323. https://doi.org/10.1016/j.procs.2015.09.089

Singh, D., & Singh, P. B. (2019). *Historical Preview of the age of Cryptography*. *7*(12).

Sultan, A., Azhar Mushtaq, M., Faheem Nazir, M., Saleem, M., Altaf, J., & Junaid, M. (2020). A new efficient encryption and decryption method using a Lossless Data Compression Scheme. *International Journal of Scientific and Research Publications (IJSRP)*, *10*(12), 583–589. https://doi.org/10.29322/ijsrp.10.12.2020.p10867

Verma, J., Shahrukh, M., Krishna, M., & Goel, R. (1760). a Critical Review on Cryptography and Hashing Algorithm Sha-512. *Www.Irjmets.Com @International Research Journal of Modernization in Engineering*, *12*, 1760–1764. www.irjmets.com