Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Symmetric, Asymmetric and Hash Functions

Louis Opoku Gyamfi
School of Technology
Ghana Institute of Management and Public Administration
GreenHills, Accra, Ghana
Email: louis.gyamfi@st.gimpa.edu.gh

ABSTRACT

Modern cryptography has become increasingly important and ubiquitous. There has been increasing concern about the security of data, as data is mostly used on computers and transmitted over networks. This increases the need to protect the data itself even more than in the past due to increasingly sophisticated attacks, a booming economy centered around computer-related crime, and data theft(Barrett & Hausman, 2011). This paper discusses two of the most common cryptographic algorithms. Hash functions are also discussed to throw light on how they are used to ensure data integrity.

Keywords : Cryptography, Cryptographic Algorithms, Symmetric Cryptography, Asymmetric Cryptography, Hash Functions, Hashing, Cryptographic Hash.

Proceedings Citation Format
Longe E.O. & Jimoh, R.O. (2022): Use & Gratification and Its Effect on the Post Adoption and Continuous Use of Mobile Payment Technologies in NigeriaMultidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 207-214. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P40

1. INTRODUCTION

Cryptography is the art of concealing information.(*Introduction to Cryptography*, n.d.). Only the sender and intended recipient of a message are able to see its contents thanks to cryptography. The term is derived from the Greek word kryptos, which means hidden. It is closely related to encryption, which is the process of converting plain text into ciphertext before sending it and then back again after receiving it. The obscuring of information in photographs using methods like microdots or merging is also covered by cryptography.(What Is Cryptography?, n.d.). The most typical use of cryptography is to encrypt and decrypt email and other plain-text messages while sending electronic data. The symmetric or "secret key" mechanism is the most straightforward approach.

Here, information is encrypted using a secret key before being transferred to the recipient for decryption along with the encoded message. The issue? A third party has all the tools necessary to decrypt and read the message if it is intercepted. (Kessler, 2019). Cryptologists created the asymmetric system, sometimes known as "public key," to solve this problem. In this scenario, each user has two keys: a public key and a private key. In order to send an encrypted communication, senders must first obtain the recipient's public key. The recipient's private key is required to decode the message when it is sent, therefore theft without the accompanying private key is useless.(Barrett & Hausman, 2011). The paper is organized in the following sections: Section 2 discusses the background of the study. Section 3 is a review of related literation. Section 4 looks at the findings of the study. Section 5 is a recommendation for policy and practice and section 6 is the conclusion of the paper.

2. CRYPTOGRAPHIC SCHEMES

Symmetric Key Cryptography

With symmetric key cryptography, the transmitter and receiver share a single secret key. Other names for symmetric key cryptography include shared-key, secret-key, one-key, and ultimately private-key cryptography. The main benefits of such a system include that it is more straightforward to implement than an asymmetric system and that it is frequently faster.

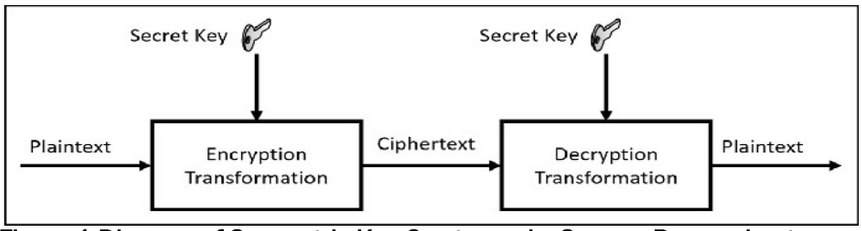

Figure 1 Diagram of Symmetric Key Cryptography Source: Researchgate.com

Symmetric encryption uses two primary types of methods for encrypting plaintext data:

Stream cipher: With a stream cipher, plaintext bits are encrypted a single bit at a time. These bits are also combined with a stream of pseudo-random characters. Stream ciphers are known for their speed and simplicity(Ahmad et al., 2015a). **Block cipher:** With a block cipher, plaintext is encrypted in blocks, which are fixed-length groups of bits. A block of plaintext is encrypted into a corresponding block of ciphertext. For example, a 64-bit block of plaintext would output as a 64-bit block of ciphertext. Because most plaintext does not fit within the precise block size, leftover text is padded to complete the block (Marty M. Weiss, 2021).

Encryption Systems Based On Symmetric Key Cryptography

Examples of symmetrical algorithms include the following:

- Advance Encryption Standard (AES): The most commonly used symmetric algorithm is the Advanced Encryption Standard (AES), which was originally known as Rijndael. Under NIST, the AES cipher has a block size of 128 bits, but can have three different key lengths as shown with AES-128, AES-192 and AES-256.
- Data Encryption Standard (DES): DES is a block cipher that uses a 56-bit key and 8 bits of parity on each 64-bit chunk of data. Although it is considered a strong algorithm, it is limited in use because of its relatively short key-length limit.

- Triple Data Encryption Standard (3DES): improves upon the DES by using the DES algorithm three times with three distinct keys.

Asymmetric Cryptography

In an Asymmetric cryptography, two key pairs are used. These keys are referred to as the private key and the public key. As the name suggests, the public key is made available to whoever will communicate with the owner of the private. The private key, however, is kept private. It is usually stored on the host system or application. There are several ways by which the public key can be made available. This includes through emails or on centralized servers that host a pseudo-address book of published public encryption keys. One challenge, however, is ensuring the authenticity of a public key. To address this, a public key infrastructure (PKI) is often used. A PKI uses trusted third parties that certify or provide proof of key ownership(Omar Santos, 2015).

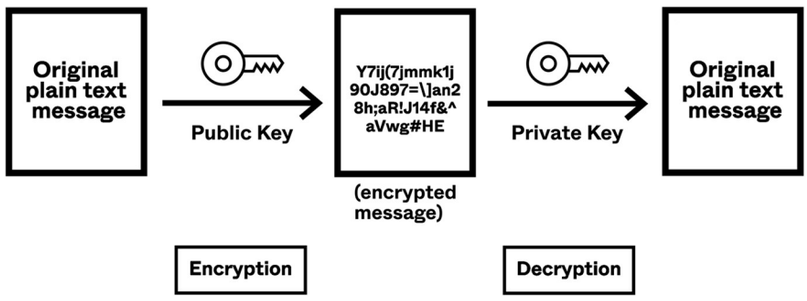

Figure 2 Asymmetric Cryptography. Source: Okta.com

Some general rules for asymmetric algorithms include the following:

- The public key can never decrypt a message that it was used to encrypt with.
- Private keys should never be able to be determined through the public key (if it is designed properly).
- Each key should be able to decrypt a message made with the other. For instance, if a message is encrypted with the private key, the public key should be able to decrypt it.
-

Encryption Systems Based On Symmetric Key Cryptography

Examples of asymmetrical algorithms include the following:

- RSA: Named after Rivest, Shamir, and Adleman, who created the algorithm. The primary use of this asymmetrical algorithm today is for authentication. It is also known as public key cryptography standard (PKCS) #1. The key length may be from 512 to 2048, and a minimum size for good security is at least 1024. Regarding security, bigger is better.
- DH: Diffie-Hellman key exchange protocol. DH is an asymmetrical algorithm that allows two devices to negotiate and establish shared secret keying material (keys) over an untrusted network. The interesting thing about DH is that although the algorithm itself is asymmetrical, the keys generated by the exchange are symmetrical keys that can then be used with symmetrical algorithms such as Triple Digital Encryption Standard (3DES) and Advanced Encryption Standard (AES).
- ElGamal (second character is an L): This asymmetrical encryption system is based on the DH exchange.(Omar Santos, 2015)

3. HASH FUNCTIONS

A hash is a summary that is created using a mathematical method or algorithm, and it is frequently used as a "digital fingerprint" to check the authenticity of files and messages. Message integrity is ensured through hashing, which also enables authentication verification (Sobti & Geetha, 2012). When a block of data is given, a cryptographic hash function converts it into a small, predetermined hash value. Being a one-way function, it should produce the same fixed-sized hash when executed on two distinct computers using the same data. Generating the same hash from a different block of data is impossible (or at least not realistically doable). Collision resistance is what we call this. Sometimes referred to as the digest, message digest, or just the hash, the hashing process yields a fixed-length, short string of data as its output (Wahome Macharia, 2021). Keyed and un-keyed hash functions are the two main categories of cryptographic hash functions. Keyed hash functions employ a secret key, whereas un-keyed hash functions do not. Message Authentication Code (MAC) is the term used to describe the keyed Hash functions (Gligoroski, 2011).

How Hashing Works

A hash function generates an output string of a set length from a string of any length, such as a password or email. A document can be used to create a hash, but the hash cannot be used to create the original document. The example that follows should make everything more understandable if this all sounds unclear. Consider sending an email to a buddy but simultaneously wanting to protect it from being read or changed while in transit. To accompany emails, you need software that creates a hash value for the message and then encrypts both the hash and the message. The recipient's program produces another hash from the received email after decrypting the message and hash when the email is received. A match between the two hashes demonstrates that the message was not altered (because any change in the original message would produce a change in the hash).

Cryptographic Hash Functions

Examples of cryptographic hash functions include the following:

- Secure Hash Algorithm (SHA, SHA-1, SHA-2, SHA-3): SHA-1 can generate a 160-bit hash from any variable-length string of data, making it very secure, but also resource intensive.
- Message Digest Series Algorithm (MD2, MD4, MD5): The MD series generates a hash of up to 128-bit strength out of any length of data.
- RACE Integrity Primitives Evaluation Message Digest (RIPEMD): developed within the academic system and is based upon the design of MD4. The more commonly used 160-bit version of the algorithm, RIPEMD-160, performs comparable to SHA-1, though it is less used.

ATTACKING HASH FUNCTIONS

Collision attacks are possible with cryptographic hashes due to their susceptibility to collisions. Such an attack looks for two input strings to a hash function that produce the same output. Although collisions are unlikely, they are possible because hash algorithms, despite accepting an infinite input length, create a predefined output length.(Marty M. Weiss, 2021). Attackers equipped with fast hardware can easily “crack” hashed credentials. MD5 and SHA-1 have been proven to contain known collisions—that is, produce the same hash value from different credentials. Rainbow tables are “optimized lookup tables” that can be used to reverse-engineer one-way hash functions.

A rainbow table is basically a pre-computed set of plaintext strings and their corresponding hashes. Large rainbow tables are publicly available, and attackers can use one of these tables to retrieve cleartext data that has been hashed (What Are Cryptographic Hash Functions? | Synopsys, n.d.).

3. REVIEW OF RELATED STUDIES

The given table presents the review of studies conducted in the context of cryptographic algorithms and hash functions.

Table 1 Review of studies conducted in context of Cryptographic Algorithms and Hash Functions

Authors	Work on Cryptographic Algorithms and Hash Functions
(Yassein et al., 2018)	This paper presents a comprehensive study between Symmetric key and Asymmetric key encryption algorithms that enhanced data security in cloud computing system. It discusses AES, DES, 3DES and Blowfish for symmetric encryption algorithms, and RSA, DSA, Diffie-Hellman and Elliptic Curve, for asymmetric encryption algorithms.
(Ahmad et al., 2015b)	This paper presents a comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets through simulation. This paper evaluates both symmetric (e.g. ESEBM: enhanced symmetric key encryption based mixnet) and asymmetric (e.g. RSA and ElGamal based) key encryption algorithm based decryption mixnets.
(Al-Shabi, 2019)	This paper discusses several important algorithms used for the encryption and decryption of data in all fields, to make a comparative study for most important algorithms in terms of speed (implementation) and security (special keys) determine whether an encryption algorithm is good. What is more, computational resources, such memory (RAM) size, are an integral consideration since they affect algorithm efficiency, hence the need to ensure optimal resource allocation, etc.
(Gupta, 2020)	The purpose of this paper is to review concepts of cryptography and cryptographic hash functions. Main concentration is on various algorithms including DES, RSA. The author also discussed cryptographic hash functions- MD family, SHA family and RIPEMD, BLAKE and WHILPOOL families.
(Wahome Macharia, 2021)	This paper describes what cryptographic hash functions are, what security properties are expected of them and what attacks can be performed against them.
(Raigoza & Jituri, 2017)	In this paper, the authors sought to evaluate the performance of symmetric algorithms. The compared the performance between the universally used Advanced Encryption Standard (AES) and Blowfish algorithms. The execution time is measured for different types of data string values. The length of the string as well as ASCII value range is also varied.
(Pujol et al., 2008)	The purpose of this paper is to propose a client/server architecture to efficiently authenticate users by means of their fingerprint biometric feature. To do this, the personal data of each user are acquired at the client and, afterwards, they are conveniently encrypted using a combination of up-to-date symmetric and asymmetric cryptographic algorithms.

4. RESEARCH FINDINGS

Although cryptography helps safeguard our networks and systems, some cryptographic algorithms are seriously threatened by the rapid advancement of technology. The ability of computers to break cryptographic techniques is increasing. Because of the amount of inertia in large commercial systems where interoperability is crucial, algorithms like DES, MD5, SHA-1, and RSA-512 are still employed in some areas but are still thought to be breakable using classical computing now or in the near future. (Quantum Computing and Its Impact on Cryptography, n.d.).

5. RECOMMENDATION FOR POLICY AND PRACTICES

Institutions must use stronger algorithms to encrypt their resources in light of the threat posed by the rapid growth of technology. Mathematicians and academics must develop algorithms that can survive the threat posed by technological breakthroughs in order to be ready for the future.

6. CONCLUSION

The rapid expansion of digital data transfer and storage depends on cryptography. It is employed to fulfill the primary security objectives of confidentiality, integrity, authentication, and nonrepudiation. A variety of cryptographic algorithms are being developed to meet these objectives. This paper's major goal is to spread knowledge about the three primary cryptographic techniques, symmetric key cryptography, asymmetric cryptography, and hash functions.

REFERENCES

1. Ahmad, S., Alam, K. M. R., Rahman, H., & Tamura, S. (2015a). A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. *Proceedings of 2015 International Conference on Networking Systems and Security, NSysS 2015*, *April 2018*. https://doi.org/10.1109/NSysS.2015.7043532
2. Ahmad, S., Alam, K. M. R., Rahman, H., & Tamura, S. (2015b). A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. *Proceedings of 2015 International Conference on Networking Systems and Security, NSysS 2015*. https://doi.org/10.1109/NSysS.2015.7043532
3. 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
4. Barrett, D., & Hausman, K. K. (2011). *CompTIA Security + Sy0-301. Authorised Exam Cram. Third Edition*.
5. Gligoroski, D. (2011). Cryptographic hash functions. *A Multidisciplinary Introduction to Information Security*, *May*, 49–72. https://doi.org/10.1587/essfr.4.57
6. Gupta, R. K. (2020). A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function. *European Journal of Molecular & Clinical Medicine* , *7*(7), 3397–3408.
7. *Introduction to Cryptography*. (n.d.). Retrieved August 10, 2022, from https://linuxhint.com/cryptography/
8. Kessler, G. C. (2019). *An Overview of Cryptography (Updated Version*. *January*, 1–65. https://www.garykessler.net/library/crypto.html
9. Marty M. Weiss. (2021). Cryptographic concepts. In Mark Taub (Ed.), *CompTIA Security+ SY0-601 Exam Cram* (pp. 489–502). Pearson Education, Inc.
10. Omar Santos, J. S. (2015). Fundamentals of VPN Technology and Cryptography. In *Official Cert Guide. CCNA Security 210-260* (pp. 83–119). Cisco Press.
11. Pujol, F. A., Mora, H., Sánchez, J. L., & Jimeno, A. (2008). A client/server implementation of an encryption system for fingerprint user authentication. *Kybernetes*, *37*(8), 1111–1119. https://doi.org/10.1108/03684920810884937
12. *Quantum Computing and its Impact on Cryptography*. (n.d.). Retrieved August 16, 2022, from https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography
13. Raigoza, J., & Jituri, K. (2017). Evaluating Performance of Symmetric Encryption Algorithms. *Proceedings - 2016 International Conference on Computational Science and Computational Intelligence, CSCI 2016*, 1378–1379. https://doi.org/10.1109/CSCI.2016.0258
14. Sobti, R., & Geetha, G. (2012). Cryptographic Hash functions - a review. *IJCSI International Journal of Computer Science Issues*, *9*(2), 461–479. https://www.researchgate.net/publication/267422045
15. Wahome Macharia. (2021). Cryptographic hash functions. *A Multidisciplinary Introduction to Information Security*, *May*. https://doi.org/10.1587/essfr.4.57
16. *What are cryptographic hash functions? | Synopsys*. (n.d.). Retrieved August 16, 2022, from https://www.synopsys.com/blogs/software-security/cryptographic-hash-functions/

17. *What is Cryptography?* (n.d.). Retrieved August 10, 2022, from https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
18. Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2018). Comprehensive study of symmetric key and asymmetric key encryption algorithms. *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, *2018-Janua*, 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308215