International Journal of
Engineering in Computer Science

E-ISSN: 2663-3590
P-ISSN: 2663-3582
IJECS 2023; 5(1): 19-22
Received: 22-10-2022
Accepted: 09-12-2022

S Priyadharsini
UG Scholar, Department of ECE, Government College of Engineering, Bodinayakkanur, Theni, Tamil Nadu, India

K Thamizhmaran
Assistant Professor & NSS Programme Officer, Department of ECE, GCE, Bodinayakkanur, Theni, Tamil Nadu, India

A study of data security using cryptography

S Priyadharsini and K Thamizhmaran

DOI: https://doi.org/10.33545/26633582.2023.v5.i1a.84

Abstract
To make better data transmission over networks cryptography is used with the internet having reached a level that merges with our lives, growing explosively during the last several decades; data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.

Keywords: Cryptography, security, algorithm, cipher, decryption, data security

Introduction

Cryptography is a technique to achieve confidentiality of messages. The term has a specific meaning in Greek: “secret writing”. Nowadays, however, the privacy of individuals and organizations is provided through cryptography at a high level, making sure that information sent is secure in a way that the authorized receiver can access this information. With historical roots, cryptography can be considered an old technique that is still being developed. Examples reach back to 2000 B.C., when the ancient Egyptians used “secret” hieroglyphics, as well as other evidence in the form of secret writings in ancient Greece or the famous Caesar cipher of ancient Rome. Billions of people around the globe use cryptography on a daily basis to protect data and information, although most do not know that they are using it. In addition to being extremely useful, it is also considered highly brittle, as cryptographic systems can become compromised due to a single programming or specification error.

Cryptography: It is the process of transforming the secret data or information into a unreadable or scrambled form. In fact it is the art of writing the message secretly. The concept of cryptography depends on five factors. These are discussed below [1].

a) **Plain text:** The message or information that we want to send secretly. The set of plain text is represented by P.
b) **Cipher text:** It is the scrambled or unreadable form of information or message. The set of cipher text is represented by C.
c) **Key:** It is the rule with the help of which data is scrambled. The set of keys is represented by **K.**
d) **Encryption Function:** It is the method using which the cipher text is generated. The set of encryption function is represented by E(x).
e) **Decryption Function:** It is the inverse function of E(x). It is the effort to generate the original message. The set of decryption function is represented by D(x).

Thus cryptography is depends on {P, C, K, E(x), D(x)}.

Literature Survey

Susan *et al.* [4] pointed out that network and computer security is a new and fast-moving technology within the computer science field, with computer security teaching to be a target that never stops moving. Algorithmic and mathematic aspects, such as hashing techniques and encryption, are the main focus of security courses. As crackers find ways to hack network systems, new courses are created that cover the latest type of attacks, but each of these attacks become outdated daily due to the responses from new security software.

Correspondence
S Priyadharsini
UG scholar, Dept. of ECE, Government College of Engineering, Bodinayakkanur, Theni, Tamil Nadu, India

With the continuous maturity of security terminology, security techniques and skills continue to emerge in the practice of business, network optimization, security architecture, and legal foundation. Othman O. Khalifa *et al.* [5] demonstrated the primary basic concepts, characteristics, and goals of cryptography.

They discussed that in our age, i.e. the age of information, communication has contributed to the growth of technology and therefore has an important role that requires privacy to be protected and assured when data is sent through the medium of communication. Nitin Jirwan*et al.* [6] referred to data communication as depending mainly on digital data communication, in which data security has the highest priority when using encryption algorithms in order for data to reach the intended users safely without being compromised. They also demonstrated the various cryptographic techniques that are used in the process of data communication, such as symmetric and asymmetric methods.

In a review on network security and cryptography, Sandeep Tayal *et al.* [7] mentioned that with the emergence of social networks and commerce applications, huge amounts of data are produced daily by organizations across the world. This makes information security a huge issue in terms of ensuring that the transfer of data through the web is guaranteed. With more users connecting to the internet, this issue further demonstrates the necessity of cryptography techniques. This paper provides an overview of the various techniques used by networks to enhance security, such as cryptography.

Anjula Gupta *et al.* [8] showcased the origins and meaning of cryptography as well as how information security has become a challenging issue in the fields of computers and communications. In addition to demonstrating cryptography as a way to ensure identification, availability, integrity, authentication, and confidentiality of users and their data by providing security and privacy, this paper also provides various asymmetric algorithms that have given us the ability to protect and secure data.

A study conducted by Callas, J. [9] referred to topics such as cryptography, privacy enhancing technologies, legal changes concerned with cryptography, reliability, and technologies used in privacy enhancement. He noted that it is how society uses cryptography that will determine the future of cryptography, which depends on regulations, current laws, and customs as well as what society expects it to achieve. He indicated that there are many gaps in the field of cryptography for future researchers to fill. Additionally, the future of cryptography relies on a management system generating strong keys to ensure that only the right people with the right keys can gain access, while others without the keys cannot. Finally, Callas indicated that people's perspectives and thoughts about security and communication privacy are a mirror of the changes that occur in laws that came into existence through events such as the terrorist attacks of September 2001.

Therefore, cryptography will always play a role in the protection of data and information, for now and in the future. Moving forward with the goals of cryptography, James L. Massey [10] pointed out that there are two goals that cryptography aims to achieve as they are: authenticity and/or secrecy. In terms of the security that it affords (which can be either practical or theoretical), he discussed both Shannon's theory of theoretical secrecy as well as Simmon's theory of theoretical authenticity.

Lastly, Schneier [11] concluded that secrecy of security as a good thing is a myth and that it is not good for security to be secret, as security completely relying on secrecy can be fragile. If that secrecy was lost, regaining it would be impossible. Schneier further expressed that cryptography based on short secret keys that can be easily transferred and changed must rely on a basic principle, which is for the cryptographic algorithms to be simultaneously strong and public in order to offer good security. The only reliable way to make more improvements in security is to embrace public scrutiny.

Varol, N. *et al.* [12] studied on symmetric encryption which is used for the encryption of a certain text or speech. In this study the content to be encrypted is first converted into an encapsulation cipher that cannot be understood by a cipher algorithm.

Chachapara, K. *et al.* [13] examined secure sharing with cryptography in cloud computing and demonstrated a framework that makes use of cryptography algorithms like RSA and AES, with AES been the most secure algorithm in cryptography. The cloud users can generate keys for different users with different permissions to access their files.

Orman, H. [14] mentioned that many discussions and developments are generated about cryptography, as the author stated the hash functions are playing a vital role in cryptography by supplying nearly number to any piece of data and by the years that MD5's weaknesses became known, it led to an unsettled feeling about how to design hash functions.

Gennaro, R. [15] discussed randomness in cryptography and explained that a random process is one whose consequences are unknown, and mentioned that this is why randomness is vital in cryptography since it provides a way to create information that an adversary cannot learn or predict it.

Preneel, B. [16] demonstrated cryptography and information security in the post-Snowden era, where he discussed mass surveillance practices and the security of ICT systems as well as known ways in which sophisticated attackers can bypass or undermine cryptography.

Sadkhan, S. B. [17] pointed to the main process and trends of the fields in cryptography the time of Julius Cesar till the modern era, as well as mentioning the current status of the Arabic industrial and academical efforts in this field in the past that is related to the existing cryptographic and search for new evaluation methods for the security of information.

Cryptography Concept

The basic concept of a cryptographic system is to cipher information or data in order to achieve confidentiality of the information in a way that an unauthorized person would be unable to derive its meaning. Two of the most common uses of cryptography would be using it to transmit data through an insecure channel, such as the internet, or ensuring that unauthorized people do not understand what they are looking at in a scenario in which they have accessed the information.

In cryptography, the concealed information is usually termed "plaintext", and the process of disguising the plaintext is defined as "encryption"; the encrypted plaintext is known as "ciphertext". This process is achieved by a number of rules known as "encryption algorithms". Usually, the encryption process relies on an "encryption key", which is then given to the encryption algorithm as input along with the information. Using a "decryption algorithm", the receiving side can retrieve the information using the appropriate "decryption key" [18].

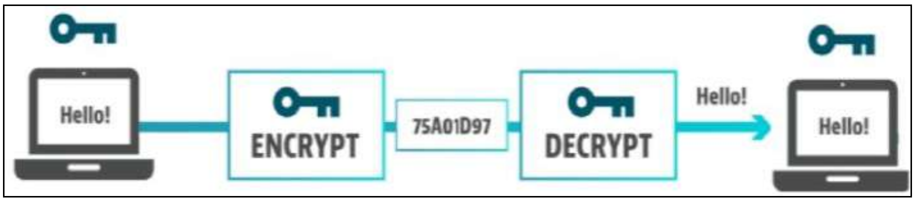

Fig 1: Encryption and Decryption

Cryptography Goal

Cryptographic goals are set before developing a new encryption model.

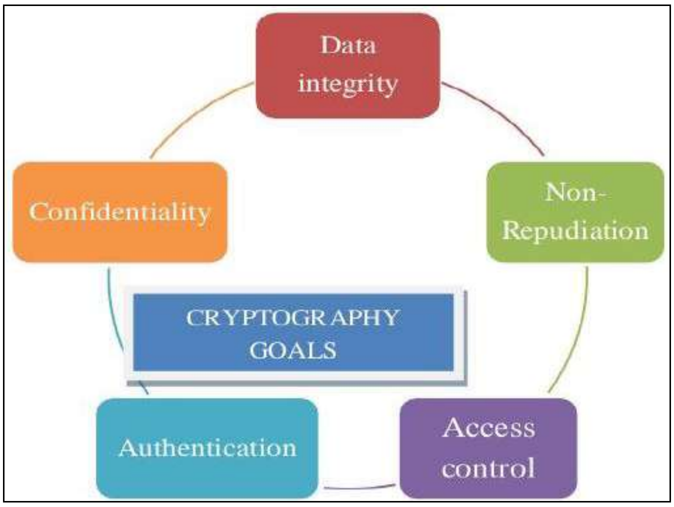

Fig 2: Goals of Cryptography

Cryptography

Integrity: Cryptography can also be used to ensure data integrity. This means that the data has not been tampered with or modified during transit or storage. Hash functions are often used to ensure data integrity. A hash function is a mathematical function that generates a fixed-size output (hash) from an input (data). The hash is unique to the input and can be used to detect any changes to the input.

Authentication: Cryptography can be used for authentication, which ensures that the individuals accessing the data or system are who they claim to be. Digital signatures are often used for authentication. A digital signature is a mathematical technique used to verify the authenticity of a digital document or message.

Non-repudiation: Cryptography can also be used to ensure non-repudiation. This means that the sender of a message cannot deny having sent the message. Digital signatures can be used for non-repudiation by providing evidence that the sender sent the message and that the message has not been altered since it was sent. Overall, cryptography is a crucial tool for ensuring the security and privacy of data and communications in various contexts

Types of Cryptography

- Symmetric key
- Asymmetric key

Symmetric key cryptography: In symmetric key cryptography, the same key is used for both encryption and decryption. This means that both the sender and receiver of a message share the same key. Symmetric key cryptography is faster than asymmetric key cryptography and is often used for encrypting large amounts of data.

Asymmetric key cryptography: Asymmetric key cryptography (also known as public-key cryptography) uses two keys - a public key and a private key. The sender of a message encrypts it using the receiver's public key, and the receiver decrypts the message using their private key. Asymmetric key cryptography is slower than symmetric key cryptography but is more secure.

Hybrid cryptography: Hybrid cryptography combines both symmetric and asymmetric key cryptography. In hybrid cryptography, a symmetric key is generated and used for encrypting the data, and the symmetric key is then encrypted using the recipient's public key. This approach is faster than asymmetric key cryptography and more secure than symmetric key cryptography.

Cryptographic hash functions: Cryptographic hash functions are used to ensure data integrity. A hash function generates a fixed-size output (hash) from an input (data). The hash is unique to the input, and any changes to the input will result in a different hash. Hash functions are often used to store passwords securely. Instead of storing the password itself, the hash of the password is stored, and when the user enters their password, the hash of the password is compared to the stored hash.

Cryptographic protocols: Cryptographic protocols are sets of rules and procedures used to ensure secure communication. Examples of cryptographic protocols include Transport Layer Security (TLS) and Secure Sockets Layer (SSL), which are used to secure internet communication.

Advantages of cryptography

- The techniques that cryptographers utilize can ensure the confidential transfer of private data.
- Techniques relating to digital signatures can prevent imposters from intercepting corporate data, while companies can use hash function techniques to maintain the integrity of data.

Disadvantages of cryptography

- A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. ...
- High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography

Conclusion

Cryptography plays a vital and critical role in achieving the primary aims of security goals, such as authentication, integrity, confidentiality, and no-repudiation. Cryptographic algorithms are developed in order to achieve these goals. Cryptography has the important purpose of providing reliable, strong, and robust network and data security. In this paper, we demonstrated a review of some of the research that has been conducted in the field of cryptography as well as of how the various algorithms used in cryptography for different security purposes work. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and ecommerce data and providing a respectable level of privacy.

References

1. Sharma Prabhjot N, Kaur H. A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science. 2017;8(Special Issue 2):323-326.
2. Preneel B. Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer; c2010.
3. Katz J, Lindell Y. Introduction to Modern Cryptography, London: Taylor & Francis Group, LLC; c2008.
4. Lincke SJ, Hollan A. Network Security: Focus on Security, Skills, and Stability, in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee; c2007.
5. Goyal. A Review paper on Network Security and Cryptography, Advances in Computational Sciences and Technology. 2017;10(5):763-770.
6. Jirwan N, Singh A, Vijay S. Review and Analysis of Cryptography Techniques. International Journal of Scientific & Engineering Research. 2013;3(4):1-6.
7. Thamizhmaran K, Santosh Kumar Mahto R, Sanjesh Kumar Tripathi V. Performance Analysis of Secure Routing Protocols in MANET. International Journal of Advanced Research in Computer and Communication Engineering. 2012;1(9);651-654.
8. Akshayadevi Arivazhagan, Thamizhmaran K, Thamilselvi N. Performance Comparison of on Demand Routing Protocols under Back whole For MANET, Advance Research in Computer science and software Engineering. 2015;5(3):407-411.
9. Prabu K, Thamizhmaran K. Cluster Head Selection Techniques and Algorithm for Mobile Ad-hoc Networks (MANETS), Advance Research in Computer science and software Engg. 2016;6(7):169-173.
10. Thamizhmaran K. Performance Evaluation of EA3ACK in different topology's Using EAACK for MANET, I - Manager Journal of information technology. 2016;5(4):5-10.
11. Thamizhmaran K, Anitha M, Alamelunachippan. Comparison and Parameter Adjustment of Topology Based (S-EA3ACK) for MANETs, International Journal of Control Theory and Application. 2017;10(30):423-436.
12. Thamizhmaran K, Anitha M, Alamelunachippan. Performance Analysis of On-demand Routing Protocol for MANET Using EA3ACK Algorithm. International Journal of Mobile Network Design and Innovation (Inderscience). 2017;7(2):88-100.
13. Thamizhmaran K. "Modified ABR (M-ABR) Routing Protocol with Multi-cost Parameters for Effective Communication in MANETs, IJARCS. 2017;8(1):288-291.
14. Thamizhmaran K, Anitha M, Alamelunachippan. Reduced End-To-End Delay For Manets Using Shsp-Ea3ack Algorithm, Journal on Communication Engineering and System. 2018;7(3):8-15.
15. Thamizhmaran K. Performance Comparison of ABR using EPKCH in MANET, I - Manager Journal of Information Technology. 2018;7(2):23-28.
16. Thamizhmaran K. Secure Three Acknowledgements Based Quality Routing Protocol for WSN. Journal of Optoelectronics and Communication (HSBR). 2020;2(3):1-5. https://doi.org/10.5281/zenodo.4042916.
17. Thamizhmaran K. RFID for Library Management System. Journal of Advance in Communication System. 2021 May;4(1):1-18. http://doi.org/10.5281/zenodo.4787338
18. Thamizhmaran K. Network Privacy Reflection using Internet of Thinks, HBRP Publication on Recent Trend in Control and Converter. 2020 June;3(3):1-11. http://doi.org/10.5281/zenodo.4477853
19. Thamizhmaran K. A Review of Vehicular Ad hoc Network Broadcasting Techniques. Journal of Sensor Research and Technologies. 2020;2(3):1-10. https://doi.org/10.5281/zenodo.4222093
20. Thamizhmaran K. EE-ATPSP – Evaluation Node Life Time for WSNs, i-manager's Journal on Wireless Communication Network. 2020 Jan-June;8(4):27-35.
21. Thamizhmaran K. Issues in Wearable Electronics Devices for Wireless Sensor Network, i-manager's Communication System and Engineering. 2020;9(1):34-38.
22. Thamizhmaran K. EEQRP-Energy Efficient Quality Routing Protocol for Wireless Sensor Networks, Journal of Signal Processing. 2017;3(1):1-6.
23. Thamizhmaran K. IOT-Fundamentals and Applications International Journal of Advance Research and Review. 2019;4(3):10-13.
24. Thamizhmaran K. Security Attacks in Wireless Sensor Networks – A Study, i-manager's Journal on Information Technology. December 2019 - February 2020;9(1):35-43.
25. Thamizhmaran K. IOT supported security considerations for network WSEAS Transactions on Communications. 2020;19:113-123. https://doi.org/10.37394/23204.2020.19.14.