DOI: 10.56452/2021SP-8-027

ISSN: 0974-5823 Vol. 6 (Special Issue 3, November 2021)

International Journal of Mechanical Engineering

A Review of Cryptography Techniques

Jyotinder Kaur[1,*] and Ruchi Sharma[2]

[1]Department of Computer Science & Engineering, Chandigarh Engineering College, Jhanjeri, Mohali-140307, Punjab, India

[2]Department of Computer Application, Chandigarh School of Business, Jhanjeri, Mohali-140307, Punjab, India

E-mail: jyotinder.j1843@cgc.ac.in

Abstract: Data security has become a major problem for anyone connected to the internet, as it has evolved to the point where it meets our health and has grown. Data security ensures that only the intended recipients have access to our information and prevents data from being tampered with or deceived. Various strategies and procedures have been established to achieve this level of safety. Cryptography is a set of encryption techniques using specific algorithms that render data invisible to the naked eye, unless they are translated using predefined data.

Keywords: Data Security, Cryptography, Security, Algorithm, Cipher, Decryption

Introduction

Cryptography is a way of securing the confidentiality of a message. In Greek, this expression has a special meaning: "hidden text." Today, however, the privacy of individuals and organizations is protected by sophisticated cryptography, which ensures that the information presented is secure and that only authorized recipients can access it [1]. Cryptography, with its historical origins, can be regarded as the most ancient form of continuous exploration. The examples date from 2000 B.C., when the ancient Egyptians used the "secret" text of hieroglyphs, as well as additional proofs such as ancient Greek cuneiform texts and the famous Caesar cipher in ancient Rome. [2].

Hundreds of millions of people use cryptography on a regular basis to protect data and information, while most do not. Cryptographic systems, besides being incredibly valuable, are also extremely smart, as a single editing or deciphering error can put them. [3].

Literature survey

Susan et al. [4] noted that network and computer security is a new and emerging technology in the field of computer science, computer security education is a moving goal. Safety studies concentrate on algorithmic and mathematical subjects such as hash algorithms and encryption. New studies covering the latest types of attacks are being published as hackers uncover new ways to penetrate network systems, but each of these attacks becomes a daily occurrence as new security software responds. Security strategies and expertise continue to emerge in operational operations, network improvement, security establishment and legal foundations of protection grows.

The basic concepts, structures, and purposes of cryptography are illustrated by Othman O. Khalifa et al. [5].

They emphasized how communications have contributed to the development of technology in our time, the information age. Therefore, it plays an important role in the need to protect and guarantee privacy when data is transmitted over communications.

DOI: 10.56452/2021SP-8-027

Data communication by Nitin Jirwan et al. [6] is primarily based on digital data transmission, where data security is a priority when using encryption techniques to ensure that data reaches target users securely and without risk. It also shows a set of cryptographic schemes, such as symmetric and asymmetric schemes, used in data communication processes.

Sandeep Taya et al. In a review of network security and encryption, [7] found that with the rise of social networking and commercial applications, organizations around the world are generating large amounts of data every day. As a result, information security is becoming a major concern when it comes to ensuring secure data transmission over the Internet. As more and more people connect online, this issue emphasizes the importance of writing a strategy. This white paper outlines many of the security measures used in your network, including encryption.

Anjula Gupta et al. [8] discussed the history and importance of cryptography and how information security has become a major concern in computing and communications environments. This document allows you to protect and protect your data in addition to displaying encryption as a means of identifying, availability, integrity, verification, and confidentiality of users and their data by providing security and privacy. We will also introduce various asymmetric algorithms to make.

Cryptography, privacy-friendly techniques, legal advances related to cryptography, reliability, and privacy-friendly techniques were all discussed in a study conducted by Callas, J. [9]. He said the future of cryptography depends on how the community uses it, the law, current laws and practices, and what the general public wants to do. He said there are many gaps in the field of cryptography that future scientists need to fill. In addition, the future of cryptography relies on management systems to create strong keys, making it accessible only to the right people with the right keys and not to those who don't. increase. Finally, Mr. Crow said that people's views and opinions on security and privacy in communications differ.

Therefore, encryption will always play a role in protecting data and information now and in the future.

James L. Massey [10] goes further with the goal of cryptography and points out that there are two goals that cryptography is trying to achieve: reliability and confidentiality. He examined both the mysterious theory of Shannon's theory and Simmons' view of the credibility of the theory it provides (either reality or theory).

After all, Schneier [11] will always keep security private, as the privacy of property security is very sensitive and only confidentiality-based security can be compromised. not. If lost, this secret cannot be recovered. To provide effective security, encryption should be based on short key-based rationale that can be quickly shared and verified, depending on which encryption method is robust and exposed. The only sure fire way to increase security is to make it publicly available.

N Varoletal. [12] I have studied symmetric encryption used to encrypt a given text or phrase. The encrypted content has been converted to an incomprehensible encapsulated Chipher encryption algorithm.

Chachapara, K. et al. [13] studied the secure sharing of cloud computing with cryptography and developed a framework using cryptographic algorithms such as RSA and AES. AES has become the most secure algorithm for encryption. Cloud users can generate keys for different users with different permissions to view files.

According to Orman, H. [14], there has been much debate and development related to encryption. As the author points out, hash functions play an important role in cryptography, assigning almost any number to any data. The days when MD5 bugs were known brought an unusual sensation to hash function design guides.

R. Gennaro [15] emphasized the irregularities of cryptography and explained that random processes have unknown consequences. Therefore, randomness is very important in encryption because it can generate information that the enemy cannot read or predict.

B. Preneel [16] investigated methods of monitoring and security of ICT systems in the post-Snowden era, as well as known methods by which complex intruders can pass or break cryptography.

Sadkhan, S. B. [17] discussed key processes and styles from Julius Caesar's time to the present, as well as the current state of past Arab industrial and educational efforts related to existing encryption and retrieval. To find a new way to test information protection.

Cryptography concept

The basic premise of an encryption system is to encrypt information and data to ensure confidentiality so that unauthorized persons can access its meaning. Two of the most common uses of encryption are sending data over insecure channels such as the Internet and understanding what unauthorized people are seeing in the context in which the data is received. It is to prevent it.

In encryption, ambiguous data is called "empty text" and the process of encrypting it is called "encryption". Clearly encrypted text is called "ciphertext". This is achieved by a set of principles called "encryption algorithms". The encryption process typically uses the "encryption key" and data provided by the encryption algorithm as input. The receiver can extract the information using an "encryption algorithm" and the required "encryption key" [18].

Historical algorithms

A. This section presents some historical algorithms and pencil and paper examples for students who are not learning math. These strategies were developed and implemented long before public key cryptography was invented.

B. Caesar Cipher

During the Gallia War, Roman emperor Julius Caesar introduced one of the oldest and oldest versions of the cipher. His letter A is encoded by the letter that precedes each letter of the alphabet in three places. In this algorithm, the remaining letters A, B, and C are represented by X, Y, and Z. This indicates that a "shift" of 3 is used, but you can get the same result in the ciphertext by choosing any number from 1 to 25. Therefore, switches are now commonly referred to as Caesar ciphers. [18].

The Caesar cipher is one of the basic events of crucifixion and is easy to crack. Deleted characters need to be restored to their original location in order to decode the text. Despite this flaw, it could have been powerful enough for Julius Caesar to use in all his past battles. However, the Caesar cipher always changes three alphabets, so anyone trying to separate the ciphertext only needs to change the letters. [19].

C. Ciphers of Simple Substitution For example, consider a simple substitution cipher commonly known as a monoalphabetic cipher. The Simple Substitution Cipher, places the characters in random order below the spelled characters, as follows:

Cryptography states that "each character is replaced by the character below it," while cryptography states that "each character is replaced by a smaller character."

D. Ciphers of Transposition Some ciphertext families use keys and specific rules to place characters in plaintext and convert them into ciphertext. Conversion is the process of converting characters to ambiguous text using specific rules and keys. Column transposed digits are one of the most basic types of transposed digits, and there are two types: "complete column transformations" and "incomplete column transformations". The rectangular shape is used to represent empty text that is written horizontally, regardless of the shape used, and its width must match the key length used.

Modern algorithms

A. Stream cyphers

Broadcast encryption uses the bits generated by the keystrokes to encrypt plaintext. Plain text is XORed by combining plain text with pseudo-random bits. Previously, stream ciphers were easier to break than block ciphers and could be circumvented. However, after many years of development, streaming cryptography has improved security and can be used for connections, Bluetooth, communications, 4G cellular, TLS connections and other applications.

Each bit of the streaming cipher is encrypted individually. One is a synchronous stream cipher, where the key flow is key dependent. The second is an asynchronous stream cipher whose ciphertext is based on key distribution. The dotted line is shown in Figure 3. Broadcast ciphers can be asynchronous if they exist. Otherwise, it will be synchronized. An example of asynchronous cypher is cypher feedback (CFB) [2].

B. BLOCK CYPHER

This type of encryption consists of two algorithms. One is for encryption and the other is for encryption.

C. The encryption method (E) and the plaintext block (P) obtain the key (K), and C is the product containing the ciphertext block. You can use C = E to specify the encryption function (K, P).

D. The encryption algorithm (D) is the distortion of the process before the plaintext P encryption was removed. P = D is an unwritten expression (K, C).

Pseudo-random ordering (PRP) is used to make block ciphers more secure. If the key is kept confidential, an attacker cannot decrypt the block cipher and calculate the output of the input. This is true as long as K's privacy and randomness have been validated from the attacker's point of view. In a broad sense, this means that an attacker cannot see the pattern of data in and out of the block cipher.

Block size and key size are often referred to as block ciphers. Their value is important for both security. 64-bit or 128-bit blocks are used for multiple block ciphers. Both foot storage and ciphertext length are small because it is important that the block does not grow too large. Block ciphers process blocks rather than bits when it comes to ciphertext length. That is, if you want to encrypt chunks of 16-bit messages and 128-bit chunks, you must first convert the messages to 128-bit chunks. The block cipher then begins processing and extracting the 128-bit ciphertext.

DOI: 10.56452/2021SP-8-027

D. HASH FUNCTION :

They are working to map unbalanced output to non-static output through a process called compression, formerly known as Random Programming Activity (PRF). However, this is not the same as compression with ZIP and .rar files. Static map instead. To be useful, the hash function must meet two requirements:

The first requirement is that it is a one-way street.

The second requirement is to be collision resistant.

Conclusion

Authenticity, integrity, confidentiality, and non-repudiation are important security principles that help enable encryption. Cryptographic algorithms have been developed to achieve these goals. The purpose of encryption is to provide reliable, robust, secure data security and network security. This document outlines some of the research in the Cryptography article and outlines how the different algorithms used for cryptography work with different security policies. Encryption continues to be used in IT and business applications to protect personal, financial, medical, and e-commerce data while maintaining adequate levels of data protection.

References

[1] N. Sharma, Prabhjot Singh, and Hardeep Kaur, "A Review of Information Security Using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.

[2] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

[3] J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC, 2008.

[4] "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.

[5] "Communications cryptography," by O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, in RF and Microwave Conference, 2004. Proceedings of RFM 2004, Selangor

[6] N. Jirwan, A. Singh, and S. Vijay, "Review and Analysis of Cryptography Techniques," International Journal of Scientific and Engineering Research, vol. 3, no. 4, pp. 1-6, 2013.

[7] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "Network Security and Cryptography: A Review Paper," Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 763-770, 2017.

[8] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672, 2014.

[9] B. Preneel, "Cryptography and Information Security in the Post-Snowden Era," IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity, Florence, 2015.

[10] Cryptography for Developers, by T. S. Denis and S. Johnson, Boston: Syngress Publishing Inc, 2007.

[11] "New directions in cryptography," IEEE Transactions on Information Theory, Vols. IT-22, no. 6, pp. 644-654, 1976. W. D. A. M. E. HELLMAN, "New directions in cryptography," IEEE Transactions on Information Theory, Vols. IT-22, no. 6, pp. 644-654, 1976.

[12] Cryptography and Network Security Principles and Practices, by W. Stallings, Prentice Hall, New York, 2005.

[13] Foundations of Cryptography Basic Tools, by O. Goldreich, Cambridge: Cambridge University Press, 2004.