Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/52/20241674

Evolution of the encryption and analysis of algorithm

Zichun Zhao

Beijing Chaoyang Kaiwen Academy, Beijing, 100020, China

2108240066@cy.kaiwenacademy.cn

Abstract. This paper examines how cryptography has developed from the ancient kingdom to the present and examines what modern humans understand by an acceptable encryption scheme. The significance of encryption is evident; it is typically present in data, banks and governments in offline procedures, or VPNs in online ones. Additionally, the research shows how cryptography manifests itself in the world and highlights the confidentiality and universality of encryption techniques. However, the article also discusses the similarities and differences between pure mathematics and cryptography. It presents the two most widely used encryption techniques in computer science, RSA and Hush, and outlines their benefits to show why these techniques are the most often used as well as how challenging it is to comprehend and apply. It also provides some advice and recommendations to achieve the purpose of improving ability.

Keywords: Encryption, computer science, algorithm, cryptography, evolution

1. Introduction

The study of safe two-way communication techniques is known as cryptography. In most cases, this occurs when one party wishes to transmit a file or message to another using a lock that no one else can unlock in order to prevent the messages from ever ending up in the wrong hands [1]. Cryptography is still essential for maintaining secrecy, safeguarding users' data, and stopping hackers from obtaining private company information. The development of cryptography has been crucial to the advancement of the internet, and this paper continues to use and expand on this topic. The most popular two techniques for encrypting communication are RSA and Hush, however each has drawbacks of its own, such as decreased speed or security. Although data encryption is currently recognised in this document, it needs to be made easier to grasp and teach because it is currently too complex. There were three phases in the history of cryptography, and each stage developed during that time [2]. This review will introduce the three periods of history of the cryptography and how modern people realize the algorithm of RSA and Hush operations are more popular. On top of that analyze the research result to give some forecasts of the algorithm and how to run it more widely and easier to understand.

2. The History of Cryptography

The earliest history of cryptography this paper can find is from “The Histories” by Herodotus [3]. It documents the wars between 499 BC to 449 BC, for example Greco-Persian Wars, the Battle of Marathon, and other famous wars. Cryptography was used in the Old Kingdom period first time; Herodotus said The Greek city-states fought many conflicts and wars with Persia against slavery and invasion. In 480 BC, the Persians secretly assembled a powerful army and prepared to launch a surprise

DOI: 10.54254/2755-2721/52/20241674

attack on Athens and Sparta. The Greek Dima latus, seeing the gathering in the Persian city of Susa, covered the letters on the boards with a layer of wax and sent them to the Greeks to inform them of the Persian plot. Finally, the Persian navy was defeated in the Gulf of Salamis near Athens.

People mention the Spartan commander sent a bent which is carved words on it, but there is no order in it to the frontline.

KGDEINPKLRIJLFGOKLMNISOJNTVWG [4]

When this paper saw this randomly ordered word, this paper can't find any details in it. But when the commander got it, and wrapped it around a stick, to find the sentence "KILL KING".

KGDEINPKLRIJLFGOKLMNISOJNTVWG

This is the earliest cryptography in the world, that is, one letter every four digits, other letters are interfering, so the ciphertext is KILLKING. However, this legend has not been verified, because the locations of the story are in Greece and Persia, but the cipher text is in English. Although that is not real, it also can be a typical cypher example to understand what cryptography is.

The most popular encryption of ancient times is the Caesar cipher, also called substitution cipher, which was used in the Roman period. It was created by Julius Caesar, and it is an encryption system used to protect important military information. The process is about letters in plaintext being shifted backward (or forward) in the alphabet by a fixed number and replaced with ciphertext. For example, when the offset is 3, all the letters A will be replaced by D, and B by E.

In plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ.

In ciphertext: DEFGHIJKLMNOPQRSTUVWXYZABC.

Until now, humans also used the Caesar cipher to program or encrypt some data. The common offsets are these:

The offset is 10: Avocat(A→K); The offset is 13: ROT13; The offset is -5: Cassis (K 6); The offset is -6: Cassette (K 7) weigh [5].

In modern times, cryptography is used in machines. Enigma machines are a sequence of rotor cipher machines that were developed and used to protect military, diplomatic, and commercial communications during the early-to-mid twentieth century [6]. It began to be used commercially in the early 1920s and was also used by the military and government of several countries, including Nazi Germany during World War II. Despite the inadequacies of the Enigma cipher machine, its encrypted files are still difficult to decipher. It led to a great advancement in the development of cryptography.

The Enigma machine is a completed cipher and decipher system. In that, there is an electrical pathway, this route causes the current to cause the rotors next to you to rotate each time you type a character, so the character entered is not the same each time. For example, when encrypting a message starting ANX..., the operator would first press the A key, and the Z lamp might light, so Z would be the first letter of the ciphertext. The operator would next press N, and then X in the same fashion, and so on.

After a short while, Alan Turing devises a new model that is based on a cryptography machine, a mathematical logic machine that abstracts human computation. This machine is the Turing machine, which is named who made it. Turing interpreted this to mean a computing machine and set out to design one capable of resolving all mathematical problems. Still, in the process, he proved in his seminal paper "On Computable Numbers, with an Application to the Entscheidungsproblem ['Halting Problem']" that no such universal mathematical solver could ever exist [7]. This is the starting point of computer science and cryptography.

The main idea of Turing machine has several of components, because it is based on assumption. It consists by TAPE, HEAD, TABLE, and State register. Each of them has own function, like TAPE is based in an infinite size of container, and the machine has an infinitely long tape divided into cells. Each cell can contain a symbol from a finite alphabet. The tape serves as the machine's memory and can be extended indefinitely as needed for the machine's operations.

Note that each part of this machine is limited, but it has a potentially infinite length of paper tape, so this machine is just an ideal device. Alan thought that such a machine would be able to simulate any computational process that a human could perform.

DOI: 10.54254/2755-2721/52/20241674

3. The Most Common Methods of Encryption in Computer Science

At the moment, the encryption is very common in our daily life. The two best examples are RSA and Hush.

First is the RSA, this encryption method was named by its inventors, who are Rivest, Shamir, and Adleman, in 1977 [8]. RSA encryption is an algorithm used in modern computing to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm that is widely used for secure data transmission. RSA relies on the computational difficulty of factoring large numbers; this task is considered "hard" in terms of computational time complexity. The core functionality of RSA in two key ways, a public key for encryption and a private key for decryption. This process can be understood as a super large number that requires two pairs of factors, one of which is public key and one is private key. The complexity depends on the decomposition of the prime number.

The applications are common in the world:

RSA is used in secure email systems and it also ensures the privacy and security of email communications.

RSA is a key part of the SSL and TLS protocols, which are used to establish secure connections between web servers and clients [9].

RSA is used to secure VPNs, which are necessary for secure remote access to networked systems.

RSA is also used to create and verify digital signatures, allowing for the authentication of digital documents and proving the identity of a particular user.

Secure Shell (SSH): RSA is often used in SSH protocols for secure remote logins and other secure network services in an insecure network [10].

Another method is Hush, whose full name is Secure Hash Algorithm, it is an encryption algorithm that provides enhanced security measures in the realm of digital communication. This is safety because, at its core, Hush is designed to safeguard data by transforming it into an unreadable format, only decipherable by those with the appropriate decryption keys [11]. in terms of performance, the Hush encryption algorithm inputs data by applying advanced encryption measures. This process will generate a unique output that anyone without the necessary decryption key cannot understand. The original data or plaintext can only be recovered through the decryption process using this key. This two-step process - encryption and decryption - ensures the confidentiality of data during transmission.

The biggest advantage of Hush is the confidentiality. The complexity of the Hush is extremely high, making it extremely difficult for unauthorized parties to break the encryption. This is due to the algorithm’s complex mathematical structure, which requires significant computational power and time to attempt decryption without the correct key.

The applications of our world contain about employing secure messaging apps to protect the privacy of user conversations. It’s also used in the financial industry for securing sensitive transactions and personal data. Furthermore, regarding healthcare, Hush provides a way to protect patient information. Governments and military organizations also use Hush encryption to protect classified information and maintain national security.

4. Conclusion

In conclusion, the history of cryptography and encryption is meaningful to humans. Until now, cryptography has frequently appeared in several events, so the importance of cryptography and encryption is obvious. In the digital era, when people are surviving in this world, the security of information is playing an important role. The constant evolution of cryptography and encryption underlines their continued importance in our increasingly digital and interconnected world. The major history of cryptography has far-reaching significance and influence on the development of human beings. Shortly, including the present, cryptography will be widely used in artificial intelligence and network communication, and I firmly believe that the two encryption methods of Hush and RSA can be more widely used in the future, but they remain in the status quo and have not been tapped out their potential.

DOI: 10.54254/2755-2721/52/20241674

References

[1] Fortinet. (2023). What Is Cryptography? Definition, Importance, Types. Retrieved from Fortinet website: https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

[2] Robin Materese. (2016, June 30). Cryptography. Retrieved from NIST website: https://www.nist.gov/cryptography

[3] Herodotus: Introduction to History, Tianjin: Tianjin People's Publishing House, 2010.01, 12-17.

[4] Wikipedia Contributors. “Cryptography.” Wikipedia, Wikimedia Foundation, 23 Oct. 2019, en.wikipedia.org/wiki/Cryptography.

[5] Rang, Wu. “Caesar cipher (one).” Rang’s Note, 23 Oct. 2010, wurang.net/caesar_cipher_a/. Accessed 29 Nov. 2023.

[6] Singh, S. (2002). The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books.

[7] Turing, A.M. (1937) On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, s2-42, 230-265.

[8] Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[9] Rescorla, E. (2001). SSL and TLS: Designing and Building Secure Systems. Addison-Wesley Professional.

[10] Barrett, D., Silverman, R., & Byrnes, R. (2005). SSH, The Secure Shell: The Definitive Guide. O’Reilly Media, Inc.

[11] National Institute of Standards and Technology. (2015). Federal Information Processing Standards Publication 180-4: Secure Hash Standard (SHS).