Instal : Jurnal Komputer

E-ISSN: 2808-683X
Edisi : Volume 16 Nomor 05 | December 2024

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index

End-to-End Encryption Security Method

Rahmayani Rahmayani[1], Habib Muharry Yusdartono[2]
[1]Universitas Sumatera Utara,[2]Habib Muharry Yusdartono

Keywords:

End-to-end
Encryption
Cryptography

ABSTRACT

Crimes such as wiretapping, data theft and other criminal acts in social media, especially in short messages are increasingly common. Several short message service companies are beginning to understand this and continue to strive to advance security features that can protect user data and privacy. One of these efforts is the development of an end-to-end encryption security method. In this article, the author hopes to be able to explain and provide a good understanding of this security method. So that it can be understood by the reader well.

Corresponding Author:
Rahmmanie98@gmail.com

INTRODUCTION

The development of computer and telecommunications technology today has experienced very rapid progress and has become a necessity, because many jobs can be completed quickly, accurately, and efficiently. In line with the development of this technology, it has increasingly changed the way people communicate. In the past, long-distance communication still used conventional methods, namely by sending letters to each other, but now long-distance communication can be done easily and quickly, namely with the existence of technology such as email, SMS (Short Messaging Service), and the internet, which is one of the most widely used telecommunications technologies. The internet has made communication more open and the exchange of information is also faster across national and cultural boundaries.[1] The ease of accessing communication media by everyone will certainly have an impact on the security of information or messages that use the communication media. Information becomes very vulnerable to being known, taken and manipulated by irresponsible parties. Therefore, a method or way is needed that can maintain the confidentiality of this information, one of which is known as cryptography.[2] One of the popular communication media is a messaging service that utilizes internet data networks that has been used by almost all levels of society such as WhatsApp Messenger (WA), Blackberry Messenger (BBM), Kakao Talk, LINE, WeChat and other messaging applications that utilize data networks. The problem then arises whether by using the "free" messaging application our messages are safe from being tapped.[3] In this case, messenger has adopted end-to-end encryption to protect user communications. However, in daily use, there are still some security and privacy issues that need to be addressed to protect users' personal information and data shared through this instant messaging application. In implementing end-to-end encryption in instant messaging applications, it is important to consider the potential and limitations. Although end-to-end

encryption provides strong protection for message confidentiality and user privacy, other aspects such as device security, encryption key management, and recipient identity verification are also important to consider. In addition, instant messaging application users should also pay attention to the privacy policies and security statements of service providers, and continue to update their applications to address potential security vulnerabilities. By understanding the potential and limitations of end-to-end encryption, and involving users, developers, and service providers, stronger and more effective security and privacy technologies can be developed in the future.[4] Threats to data privacy on the internet can come from various sources and in various forms, such as malware, phishing, ransomware, and Distributed Denial of Service attacks. These threats not only result in financial losses but also damage the reputation and trust of users in digital systems. Therefore, it is important to understand and categorize the various types of threats that exist in order to develop effective mitigation strategies.[5] Frequent tapping and cloning when sending or forwarding information via WhatsApp often causes people to receive hoax information. Therefore, a good method of securing information delivery is needed so that the information sent is only received by the right recipient.[6] In the process of sending data (messages) there are several things that must be considered, namely: confidentiality, data integrity, authentication and non-repudiation. Therefore, a message encoding or coding process is needed before the sending process is carried out. So that the message sent is kept confidential and cannot be easily changed to maintain the integrity of the message.[7] The science that studies data security methods is known as Cryptography, while the steps in cryptography are called cryptographic algorithms. Based on the key used, cryptographic algorithms can be divided into two, Symmetric Algorithms and Asymmetric Algorithms. Where Symmetric Algorithms use one key for the encryption and decryption process. While the Asymmetric Algorithm uses two different keys for the encryption and decryption process, namely the public key used for the encryption process, namely changing the original text data (plain text) into secret text (cipher text) which is not confidential, and the private key used for the decryption process, namely returning secret text data (cipher text) to the original text (plain text) which is confidential and each party has a different private key.[8]

METHODS

A. Encryption and Description

Encryption is a message encoding technique (message/plaintext) so that the message is sent will not be the same as the original message written (message/plaintext). So what orders are still in process? This message is called ciphertext. Ciphertext is the result of encryption and messages. This secret is not the same as the original message from message sender. messages in transit (ciphertext) is a message that is not the same as the initial message sender (message/plaintext), how is the recipient can read the sender's complete message? Key or the key is needed to reveal the secret message (ciphertext). The process of changing secret messages (ciphertext) into a complete message (message/plaintext) is called the decryption process. Back to the key terms, the key used in the Caesar Cipher must be the same (symmetrical) between the sender of the message and the recipient messages used in encryption and decryption message. Here the author will not discuss further regarding key types, other cryptographic algorithms, and so on, broader cryptography.[11]

Based on the analysis of specialized journal literature on cybersecurity and data protection, we can conclude that encryption methods with a frequency of use of up to 90% are the most commonly used to protect privacy. Encryption is widely considered a very effective technique for protecting sensitive data by converting it into a format that cannot be read without the appropriate decryption key.[12] In addition to encryption, the use of access control methods is also high (80%) due to the importance of limiting data access to only authorized persons or

systems. Data anonymization methods are in second place with a frequency of use of 75%, indicating an increasing focus on protecting the identities of people in the data set. Auditing and monitoring are also commonly used (70%) to detect and respond to security incidents by monitoring data access and modification activity. Finally, tokenization is used 60% to reduce the risk of data theft, especially in the context of financial transactions. Overall, encryption and access control are the dominant methods and are often cited in the literature as the most important approaches to protecting privacy in cybersecurity. Data anonymization, auditing and monitoring, and tokenization also play an important role in data protection strategies, although less frequently than encryption and access control.[5]

B. Encryption Process
The steps in the encryption process are as follows
Plaintext is converted into numbers.

1. To convert plaintext in the form of letters into numbers, the ASCII code in the decimal number system can be used.
2. Plaintext m is expressed as blocks x1,x2,x3,. ,such that each block represents a value in the interval [0, n-1], so that the transformation is one to one.
3. Each mi block is encrypted into a ci block with the formula yi = xi PK mod r. [13]
4. Decryption Process

The steps in the decryption process are as follows:
1. Each ciphertext block yi is decrypted back into block xi with the formula

$$xi = yi\ SK \bmod r$$

2. Then the blocks m1,m2,m3,...., are changed back into letter form by looking at the ASCII code of the decryption result.[14]

C. Strength and Security of RSA
The inventor of the RSA algorithm suggested that the values of p and q be more than 100 digits long. The effort to find the factors of a 200-digit number requires a computing time of 4 billion years! (assuming that the factoring algorithm used is the fastest algorithm currently available and the computer used has a speed of 1 millisecond).Fortunately, the most effective algorithm for factoring large numbers has not been found. This is what makes the RSA algorithm still used today. As long as an effective algorithm for factoring integers into their prime factors has not been found, the RSA algorithm is still recommended for encrypting messages.[8]

RESULTS AND DISCUSSION

A. Encryption and Description

Encryption is a message encoding technique (message/plaintext) so that the message is sent will not be the same as the original message written (message/plaintext). So what orders are still in process? This message is called ciphertext. Ciphertext is the result of encryption and messages. This secret is not the same as the original message from message sender. messages in transit (ciphertext) is a message that is not the same as the initial message sender (message/plaintext), how is the recipient can read the sender's complete message? Key or the key is needed to reveal the secret message (ciphertext). The process of changing secret messages (ciphertext) into a complete message (message/plaintext) is called the decryption process. Back to the key terms, the key used in the Caesar Cipher must be the same (symmetrical) between the sender of the message and the recipient messages used in encryption and decryption message. Here the author will not discuss further regarding key types, other cryptographic algorithms, and so on, broader cryptography.[11]

Based on the analysis of specialized journal literature on cybersecurity and data protection, we can conclude that encryption methods with a frequency of use of up to 90% are the most commonly used to protect privacy. Encryption is widely considered a very effective technique for protecting sensitive data by converting it into a format that cannot be read without the appropriate decryption key.[12] In addition to encryption, the use of access control methods is also high (80%) due to the importance of limiting data access to only authorized persons or systems. Data anonymization methods are in second place with a frequency of use of 75%, indicating an increasing focus on protecting the identities of people in the data set. Auditing and monitoring are also commonly used (70%) to detect and respond to security incidents by monitoring data access and modification activity. Finally, tokenization is used 60% to reduce the risk of data theft, especially in the context of financial transactions. Overall, encryption and access control are the dominant methods and are often cited in the literature as the most important approaches to protecting privacy in cybersecurity. Data anonymization, auditing and monitoring, and tokenization also play an important role in data protection strategies, although less frequently than encryption and access control.[5]

B. Encryption Process

The steps in the encryption process are as follows

Plaintext is converted into numbers.

1. To convert plaintext in the form of letters into numbers, the ASCII code in the decimal number system can be used.
2. Plaintext m is expressed as blocks x1,x2,x3,. ,
3. such that each block represents a value in the interval [0, n-1], so that the transformation is one to one.
4. Each mi block is encrypted into a ci block with the formula yi = xi PK mod r. [13]
5. Decryption Process

The steps in the decryption process are as follows:

1. Each ciphertext block yi is decrypted back into block xi with the formula xi = yi SK mod r

2. Then the blocks m1,m2,m3,...., are changed back into letter form by looking at the ASCII code of the decryption result.[14]

C. Strength and Security of RSA

The inventor of the RSA algorithm suggested that the values of p and q be more than 100 digits long. The effort to find the factors of a 200-digit number requires a computing time of 4 billion years! (assuming that the factoring algorithm used is the fastest algorithm currently available and the computer used has a speed of 1 millisecond).Fortunately, the most effective algorithm for factoring large numbers has not been found. This is what makes the RSA algorithm still used today. As long as an effective algorithm for factoring integers into their prime factors has not been found, the RSA algorithm is still recommended for encrypting messages.[8]

D. End-to-end Encryption

End-to-end encryption technique is message encryption techniques used when the message will be sent and returned. It is decrypted when the message reaches its destination (recipient). With encryption techniques end-to-end, packets are encrypted once at the original encryption source and then decrypted only to the final destination of decryption.[3] In an effort to answer questions about the end-to-end encryption mechanism in instant messaging applications, an analysis of seven relevant literatures has been conducted. The results of the analysis show that the end-to-end encryption mechanism in instant messaging applications uses asymmetric, symmetric, or hybrid encryption with a pair of public and private keys. In the message sending process, the public key functions to encrypt the message, while the private key is used to decrypt the message. In this process, when a user sends a message via an instant messaging

application, the message is encrypted using the recipient's public key. After going through the application server, the encrypted message is received and then decrypted with the private key stored on the recipient's device. Only the recipient's device that has the private key can decrypt and understand the message in its original form. This end-to-end encryption mechanism effectively prevents third parties from intercepting messages, including communication service providers and attackers who may be on the network. The encryption keys that guarantee the security of these messages are stored on the devices that communicate with each other. With an end-to-end encryption system that uses public keys, intermediary servers, such as ISPs or other companies, are unable to intercept the contents of the message. This is because they may have the public key, but they do not have the private key needed to decrypt the message. This public key, to ensure its authenticity, is usually accompanied by a certificate that has been validated by a certificate authority (CA). Since the CA's public key is widely known and trusted, the certificate issued and signed by the CA is considered authentic. This helps ensure that the public key used is genuine and associated with the correct identity. Thus, the end-to-end encryption mechanism ensures. that messages sent between users in an instant messaging application are strictly protected from potential eavesdropping threats. Stages of end-to-end encryption. [4]

End To End Encryption Method
a. Public Key Type
1) Identity Key Pair is a long-term Curve25519 key pair
2) Signed Pre Key is a medium-term Curve25519 key pair,
generated during the application installation process, and will change in a certain time.
3) One-Time Pre Keys is a series of Curve25519 key pairs that are used only once, generated during the installation process, and will appear when needed.[15]

CONCLUSION

Based on the description above, the author can draw the following conclusion: that the security feature with end-to-end encryption techniques increases user privacy in communicating with others.

REFERENCES

[1] V. Yuniati, I. Gani, and A. Rachmat, File ARTICLE INFORMATION A B S T R A K," 2020

[2] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," Jurnal Teknologi Terpadu, vol. 4, no. 1, 2018.

[3] J. Jamaluddin, R. J. Simamora, and K. Sitepu, "Jurnal STINDO PROFESIONAL," 2016.

[4] Y. Sri Maharani, S. Trisdiatin, M. Rafli Ihsanuddin, and F. Rahma, "SEMIOTIKA Seminar Nasional Teknologi Informasi dan Matematika Kekuatan Enkripsi End-to-End: Kajian Literatur Mengenai Kerahasiaan Komunikasi Digital dalam Aplikasi Pesan Instan," 2023.

[5] Y. A. Ramadhan and R. Renaldy, "Analisis Ancaman, Metode dan Mitigasi dalam Keamanan Privasi Data di Internet," Seminar Nasional Informatika-FTI UPGRIS, vol. 2, 2024.

[6] S. PROFESIONAL Jurnal Ekonomi, B. dan Teknologi, L. Juliana Pangaribuan, and D. Sitanggang, "Keamanan Pesan Whatsapp Menggunakan Kriptografi Algoritma Government Standard (Gost)".

[7] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File 31 Oleh : Rinmar Siringoringo Analisis dan Implementasi

Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File Article Information A B S T R A K," 2020.

[8] "12009-23844-1-SM".

[9] F. Fahrianto and A. Kitanggi, "Penerapan End-To-End Encryption Dengan Metode Super Encryption Untuk Kerahasiaan Citra Digital Pada Aplikasi Instant Messaging," vol. 9, no. 1, 2016.

[10] S. P. Lestari et al., "JURNAL MEDIA INFORMATIKA [JUMIN] Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp." [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jumin

[11] K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, "Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp," Januari, vol. 2, no. 1, p. 6, 2023, doi: 10.47233/jppie.v2i1.660.

[12] N. M. Milati, "Application of Picture Media to Improve Students' English Present Continuous Tense Speaking Ability," Jurnal Pendidikan Bahasa Inggris Undiksha, vol. 9, no. 3, pp. 333–338, 2021, doi: 10.23887/jpbi.v9i3.4.

[13] "12009-23844-1-SM".

[14] "12009-23844-1-SM".

[15] P. Studi Informatika and S. I. Tinggi Teknologi Dumai Jl Utama Karya Bukit Batrem Dumai, "Gellysa Urva."