Bigint Computing Journal
Open Access
Publisher Ali Institute of Research and Publication

Effectiveness of Text Messages Using Substitution Ciphers and Transposition Ciphers

Efektivitas Pesan Teks Menggunakan Sandi Substitusi dan Sandi Transposisi

Disnu Panggabean, Siti Aisyah Hasibuan*, Yuda Fakhri Roza

Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Indonesia

A B S T R A C T

The rapid development of communication technology has brought many benefits. One technique that is always used is news channels. Currently, chat applications are widely used, everyone uses messaging applications as a communication tool to send accurate information, and everyone is increasingly satisfied using these applications. Technology has emerged to convey messages from sender to recipient more efficiently. Message content; He; Security, social, education and work and recreation. This article explains how effective text-based message security is using substitution and transposition cryptographic methods. With the introduction of encryption processes, interception of text messages should be minimized. Of these two methods, the performance test results show that all combinations of encryption and decryption are truly successful in returning the ciphertext to its original plaintext.

Keyword: Classical Cryptography, Substitution, Transposition

A B S T R A K

Perkembangan teknologi komunikasi yang pesat telah membawa banyak manfaat. Salah satu teknik yang selalu digunakan adalah saluran berita. Saat ini, aplikasi pesan instan banyak digunakan; hampir setiap orang memanfaatkan aplikasi pesan sebagai alat komunikasi untuk mengirimkan informasi secara akurat, dan tingkat kepuasan pengguna terhadap aplikasi ini semakin meningkat. Teknologi telah berkembang untuk menyampaikan pesan dari pengirim ke penerima dengan lebih efisien. Isi pesan bisa mencakup aspek keamanan, sosial, pendidikan, pekerjaan, hingga hiburan. Artikel ini menjelaskan seberapa efektif keamanan pesan berbasis teks dengan menggunakan metode kriptografi substitusi dan transposisi. Dengan penerapan proses enkripsi, penyadapan terhadap pesan teks diharapkan dapat diminimalkan. Berdasarkan pengujian performa, kedua metode ini menunjukkan bahwa semua kombinasi proses enkripsi dan dekripsi berhasil mengembalikan ciphertext menjadi plaintext aslinya dengan baik.

Kata Kunci: Kriptografi Klasik, Substitusi, Transposisi

* Correspondence :
Siti Aisyah Hasibuan,
Universitas Islam Negeri Sumatera Utara
Email: aisyahhasibuan06@gmail.com
DOI: https://doi.org/10.55537/bigint.v2i1.578
ISSN: 3032-5374
Received: 2023-01-05; Revised: 2023-01-26; Accepted: 2023-01-26

1. INTRODUCTION

The increasingly advanced development of technology has changed the way humans communicate. In the past, communication was carried out directly or face-to-face. Today, this process has shifted through innovations in digital technology that allow communication to occur via text. Many platforms, such as social media applications, have embedded chat features to support this form of interaction, as discussed in studies on cryptographic messaging techniques [1].

Along with communication growth, the development of information security systems has become a critical aspect of protecting data. Techniques such as encryption and steganography are frequently applied to ensure that data is transmitted securely. According to research in the field of educational and communication technology, these methods are often used together to strengthen the protection of information systems [2], while cryptographic foundations continue to play an important role in security applications [3].

As technology advances, so do the risks associated with it. There is growing concern that unauthorized individuals may attempt to intercept or exploit digital communications. Research on file encryption and secure transmission systems confirms that these vulnerabilities are real and must be addressed using effective countermeasures [4]. This leads to a fundamental question about whether message content transmitted through modern messaging applications can be kept safe from eavesdropping.

Cryptography is an algorithmic method that protects the confidentiality of messages by scrambling messages into unintelligible sequences. Encryption has two processes, namely encryption and decryption. Plaintext: is the first original message created by the user. Ciphertext: is the second form of a message, namely one that has been changed in form so that it is safe and cannot be read[4].

To respond to this challenge, several cryptographic algorithms have been developed. Among them, substitution ciphers and transposition ciphers are widely known as part of classical cryptography. These two methods manipulate message content either by replacing characters or rearranging their positions, as explained in studies focused on message encryption using traditional algorithms [5]. These approaches offer a level of protection that can enhance confidentiality in communication systems used by individuals or institutions [6]. Cryptography is the work or science of protecting information security. The concept of cryptography varies from past to present. In general, there are two types of cryptography, namely traditional/classical and modern [6], [7].

This study aims to evaluate the use of substitution and transposition ciphers in securing text-based communication. Studies that applied substitution methods such as the Caesar cipher in chat-based applications have shown promising results in protecting messages [7]. Other research has tested combinations of classical ciphers and found success in restoring ciphertext back to its original plaintext, which provides useful insights into their practical effectiveness [8]. Cryptography is the science that studies how data or messages are secured when sent from sender to recipient without being intercepted by third parties [8], [9]. By exploring both individual and combined implementations, this study will assess how well these methods perform in different communication contexts.

2. METHODOLOGY

The descriptive method is a research method that shows current problems and aims to describe what happened during the research. Descriptive research is intended to describe the topic or subject matter of the research in depth, precisely and in detail. The data collected and analyzed are all taken from literature and other documentary materials such as journal articles and other relevant media. The data that will be obtained in this research is secondary data and primary data [2].

Actions are carried out systematically to collect, process and decide information through certain methods/techniques to find answers to the problems to be researched.

Mirshad describes four library research activities, namely:

1) Capture insights about the "research problem" in each research discussion obtained from literature and sources and/or the latest insights about the "research problem".
2) Integrate all knowledge, both theory and new knowledge
3) Analyze several insights from various readings according to the weaknesses, strengths of each source, or the relationship of each discourse discussed in them.

4) Criticism, expressing ideas that are critical of previous discourse which presents new insights in sharing ideas about different "research problems".

Therefore, library research activities consist of collecting, reading and preserving literature/books [3].

3. RESULTS AND DISCUSSION

Encryption, decryption and cipher are important terms in cryptography with the following meanings:

1) Encryption: Encryption is a method of changing data into code patterns that cover user-generated data. The algorithm is used to encrypt data before the recipient sends back the encrypted data with the decrypted key.
2) Description: the opposite of cryptography, is a step or mechanism to scramble messages that were previously unintelligible into messages that can be understood with certain codes/methods. By using the decryption key, the original message can be recovered.
3) Ciphers: Cipher is an algorithm for performing encryption and the reverse of decryption, several specified steps are followed as a procedure.

1. Substitution ciphers

The security process involves changing the ciphertext with vertical reading. other characters contained in the text. The replaced characters can be numbers or letters. For Caesar cipher to encrypt text is to move the letters in alphabetical order, monoalphabetic encryption does not do that.

The process of protection by changing the signs contained in the character. Randomize password letters:

Here, the password replacing the original letters is random. The most important thing is the order of the letters[10].

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	H	Z	S	J	A	I	B	Q	C	R	M	K	E	L	G	D	N	F	Y	P	O	V	U	X	W	T

Plaintext : SENDIRI

Chippertext : YALJCFC

Key : Shift 7

In the example above, wildcards or ciphers are collected randomly without a particular pattern, so the key for this type of encryption is a series of all wildcards. So if the key is lost, it is very difficult to break the encryption because the possibilities are so many and there is no particular pattern.

2. Cipher transposition

Transposition is a security process consisting of changing the location or position of a sign and returning the message data to its original form. Just place the characters as they were before they were moved.

Another definition of cipher transposition is the technique of transposing or rotating each text character using a certain pattern. The principle of transposition is the opposite of substitution, where the character's place is simply replaced by another character, while transposition itself does not replace a character but changes its position.

The principle of operation of the encryption implementation is shown in the figure below, the plaintext is written horizontally with a length of 3 characters, and the ciphertext is obtained by reading it vertically.

A	K	U
D	A	N
K	A	U

Plaintext : AKU DAN KAMU

Chippertext : ADKKAAUNU

3. Effectiveness of Text Messages Using Substitution Ciphers and Transposition Ciphers

The data source for this research is an example of a WhatsApp chat, below in Figure 1.

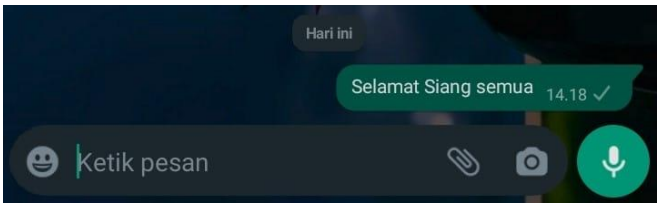

Figure 1. WhatsApp Chat Data Source

4. Encryption

Substitute Cipher with Key Shift 3 to the right, as in the table below:

Plaintext:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ciphertext:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Looking at the data source in Figure 1 and the arrangement of the letters above, the following cipher text is obtained:

Plaintext : Selamat Siang Semua

cipher text : Vhodpdw Vldqj vhpxd

The final step is encryption to obtain Cipher text 2 from Cipher text 1 with horizontal transposition whose character area is 5

Ciphertext 1 : Vhodpdw Vldqj vhpxd

V	h	o	d	p
d	w		V	l
d	q	j		v
h	p	x	d	

Viewed vertically, you will get cipher text 2 as follows:

Ciphertext 2: Vddhhwqpo jxdV dplv

Both processes are briefly described in Table 1 Consequences:

Table 1. Combination Method

Plaintext		
Selamat Siang semua		
Method	Ciphertext 1	Ciphertext 2
Substitution	Vhodpdw Vldqj vhpxd	
Transposition		Vddhhwqpo jxdV dplv

Cipher substitution will go through an encryption process starting with Key Shift 3 to the right, as in the Substitution table above as follows:

Plaintext : Selamat Siang semua

Ciphertext : Vhodpdw Vldqj vhpxd

Cipher Transposition, this encryption process will start with a horizontal transposition whose character width is 5

Plaintext : Selamat Siang semua

S	e	l	a	m
a	t		S	i
a	n	g		s
e	m	u	a	

Viewed vertically, the cipher text is obtained as follows:

Ciphertext :Saaeetnml guaS amis

5. Description

Substitution and Transposition: this description stage will begin with a description of Transposition and end with a description of Substitution

Cipher Transposition Stage to reverse cipher text 2 into cipher text 1, the process is as follows:

Ciphertext 2: Vddhhwqpo jxdV dplv

V	d	d	h
h	w	q	p
o		j	x
d	V		d
p	l	v	

Read vertically, to obtain cipher text 1:

Ciphertext 1: Vhodpdw Vldqj vhpxd

Cipher substitution is the final step, namely turning Cipher text 1 into Plaintext, with Key Shift 3 to the left, as follows:

Chiphertext:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Plaintext:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Chipher text 1 : Vhodpdw Vldqj vhpxd

Plaintext : Selamat Siang semua

Cipher substitution, in this step will start with Key Shift 3 to the left, as in the Substitution table above as follows:

Cipher text1 : Vhodpdw Vldqj vhpxd
Plaintext : Selamat Siang semua

Cipher Transposition, in this encryption stage the wide horizontal transposition of characters is 4.

Cipher text : Saaeetnml guaS amis

S	a	a	e
e	t	n	m
l		g	u
a	S		a
m	i	s	

Read vertically, the Plaintext is obtained like this:

Plaintext : Selamat Siang semua

6. Comparison of Method Effectiveness

The two methods used are substitution and transposition, compared with their efficiency, measured by the file ratio and the time required to complete the cryptographic process for each combination of methods. Cryptool software was used as a research tool to measure file size and processing time. The results obtained by the software are shown in the Table below:

Table 2. Comparison of Method Effectivenes

Combined Methods	File ratio	Duration	Results
Substitution & Transposition	9 Kb	00:01:38	Success
Substitution	4 Kb	00:00:35	Success
Transposition	5 Kb	00:01:41	Success

This research examined the effectiveness of classical cryptographic methods, specifically substitution and transposition ciphers, applied to text-based messages. The encryption and decryption processes were tested using

a WhatsApp chat sample, and each method was evaluated based on accuracy, processing duration, and file size. The results indicate that all methods successfully restored ciphertext to its original plaintext form.

7. Substitution Cipher Method

The substitution cipher was implemented using the Caesar cipher with a shift key of 3 characters to the right. In this process, each letter in the plaintext is replaced by another letter located three positions ahead in the alphabet. For instance, the plaintext "Selamat Siang semua" becomes "Vhodpdw Vldqj vhpxd" after encryption.

This method demonstrated high efficiency with a short encryption time of 00:00:35 and a small resulting file size of 4 Kb, as presented in Table 2. The findings are consistent with the study by Widiyanto et al. [10], which highlighted the Caesar cipher's simplicity and effectiveness for basic message encryption scenarios. It offers a fast and lightweight solution when minimal computational resources are preferred.

8. Transposition Cipher Method

In the transposition cipher method, the security mechanism relies on rearranging the characters in the message without altering the characters themselves. The encryption process writes the message into rows with a specified column width and then reads the message vertically to form the ciphertext. Using a block width of 4, the plaintext "Selamat Siang semua" is transformed into the ciphertext "Saaeetnml guaS amis".

Compared to substitution, this method required more processing time at 00:01:41 and resulted in a slightly larger file size of 5 Kb. This observation supports Usman's findings [5], which noted that transposition methods, while still reliable, tend to involve greater computational complexity due to character reordering.

9. Combination of Substitution and Transposition

The combination of both methods began with substitution encryption, followed by horizontal transposition. This multi-layered approach created a more complex ciphertext, such as "Vddhhwqpo jxdV dplv", which was later reversed using the inverse of each method during decryption.

This combined method required 00:01:38 of processing time and produced a 9 Kb file. Although it involved greater computational cost compared to the individual methods, it provided stronger data protection. This aligns with the study by Maricar and Sastra [1], which demonstrated that combining classical ciphers can improve resistance against cryptanalysis and increase encryption complexity.

10. Comparative Effectiveness

A comparison of all three approaches is shown in Table 2. The substitution method was the fastest and produced the smallest file, making it suitable for scenarios requiring efficiency and minimal resource use. The transposition method, while slower, offered an alternative encryption path without modifying characters. The combined method, although heavier in processing and storage, resulted in the most secure outcome, suitable for communication that requires enhanced confidentiality.

This pattern reflects findings by Pabokory et al. [4], who emphasized selecting encryption methods based on the operational needs of a system. Simpler ciphers are ideal for rapid and low-resource environments, while layered encryption approaches are recommended for higher-security applications.

4. CONCLUSION

The survey conducted showed the results of the three combinations of methods discussed, it was found that encryption and decryption were successful. Performance comparison using two metrics, file ratio and processing duration. Regarding the file ratio, the resulting large file size results from a combination of substitution and transposition methods with a file ratio of 9 kb. The smallest file ratio is the replacement method which has a file size of 4 KB. In terms of processing time, the combination of substitution and transposition methods is the longest result with a duration of 1.38 seconds. The fastest duration is the replacement method with a duration of 0.35 seconds.

REFERENCES

[1] M. A. Maricar and N. P. Sastra, "Efektivitas pesan teks dengan cipher substitusi, Vigenere cipher, dan cipher transposisi," Majalah Ilmiah Teknologi Elektro, vol. 17, no. 1, pp. 59–64, Jan. 2018, doi: 10.24843/mite.2018.v17i01.p08.

[2] D. Lestari, "Peran guru dalam meningkatkan perkembangan sosial anak usia dini," PAUD Lectura: Jurnal Pendidikan Anak Usia Dini, vol. 4, no. 2, pp. 1–7, Apr. 2021, doi: 10.31849/paud-lectura.v4i02.5315.

[3] M. Sari, "Penelitian kepustakaan (library research) dalam penelitian pendidikan IPA," Natural Science: Jurnal Penelitian Bidang IPA dan Pendidikan IPA, vol. 6, no. 1, pp. 41–53, 2020.

[4] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi kriptografi pengamanan data pada pesan teks, isi file dokumen, dan file dokumen menggunakan algoritma Advanced Encryption Standard," Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, vol. 10, no. 1, pp. 20–27, 2016, doi: 10.30872/jim.v10i1.23.

[5] A. Usman, "Teknik transposisi dalam pengamanan pesan teks," in Prosiding Seminar Nasional Teknologi Informasi dan Komputer, 2020, pp. 209–216.

[6] A. Hidayati, "Pengembangan aplikasi kriptografi dengan Caesar cipher dan Advanced Encryption Standard (AES) untuk file teks," in Prosiding, 2015, pp. 213–222.

[7] Y. D. Putri, M. Harahap, and R. R. Fauziah, "Penerapan kriptografi Caesar cipher pada fitur chatting sistem informasi freelance," Jurnal Teknologi dan Sistem Informasi, vol. 2, no. 2, pp. 87–94, 2019.

[8] H. Hamdani, "Implementasi kriptografi pada jaringan komputer," Jurnal Ilmu Komputer, vol. 7, no. 2, pp. 70–74, 2012.

[9] W. Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed. Upper Saddle River, NJ, USA: Pearson Education, 1998.

[10] S. Widiyanto, M. A. Hasan, and R. Hidayat, "Pengamanan pesan teks menggunakan kriptografi klasik metode shift cipher dan metode substitution cipher," Jurnal Teknologi Informasi dan Komputer, vol. 7, no. 1, pp. 9–17, Jan. 2021.